Privacy Commissioner
Te Mana Mātāpono Matatapu

Proactive Release:

Part 2

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.

Once our Biometric data is stolen, we are toast. Why risk it?

Thank you.

As Kiwi I firmly against the concept of using Biometrics information of any sort to identify or associate private citizens whether it be by governments private institutions.

As mentioned in the "Biometric Processing Privacy Code: consultation paper" their are simply too many cases where this information can misused or compromised.

"biometric systems can also enable pervasive surveillance, aid decisionmaking with serious consequences, continuously monitor people, target advertisements based on how you look or move or employ machine-learning to work out things about you that are deeply private.
• And biometric systems process information which is inherent to you – how you look and behave and sound – it is you.
• Biometric systems often take agency away from people. They can collect information without people's knowledge and use it to produce outputs that people have no control over and can find difficult to challenge.
• They've historically demonstrated bias and accuracy issues and, while systems have improved, if not deployed correctly or with the right settings, they can still produce inaccurate results and have discriminatory impacts."

These are not the only risks, government agencies not just in NZ but worldwide have terrible track records with maintaining and keeping confidential peoples personal information.
Data breeches that contain peoples Biometrics information would be a cat that cannot be put back in the bag once its out.

There should be no code on how this information is used and managed it should be flat out banned in both the private and public sectors because the risks to peoples identity, privacy and anonymity are simply too high.

All authoritarian governments and dictatorships start with leaders claiming to have the peoples best interests at heart, this situation is no different and should be avoided at all costs.

One need look no further than the vaccine pass system that was introduced in NZ during COVID for an example of this. It was done with the best of intentions but will ultimately be looked back on as a complete violation of peoples human rights and autonomy. With Biometrics integrated into such as system there would be no concept of privacy or indeed freedom anymore.

I would like to provide the following feedback on the Code:

1. I feel strongly that people should not be forced into allowing use of their biometric data. There should be alternatives available and there should be law in place to prohibit companies, employers and organisations from forcing people to comply against their will. There are other successful, legitimate ways that people can identify themselves, such as passports, driver licences and identity cards which can be used.
2. Do we really need this? Society has functioned perfectly well without biometrics for a long time. "Convenience" is not a strong enough argument for introducing such invasions of privacy.
3. How will this information be kept secure and not onsold or used for purposes other than which it was collected? The public cannot be expected to just trust the collectors of data. If there is a data breach, which frequently seems to have happened in the past, what will the repercussions be? How will securing

of data be policed? Anyone can say they won't abuse your data - but they do. How could this be stopped. There need to be massive penalties for leaking, onselling or otherwise abusing of data. There also need to be agencies to monitor and police data protection in a stringent manner.
4. Section 7 says that an agency can breach privacy for "public safety or concern." What does this look like? There needs to be detailed descriptions of what this means. Anyone could say they felt public safety was at risk for the flimiest of reasons. This should be tightened up much more so agencies and the public are crystal clear about it.
5. Section 8 says that agencies can use someone's data if they believe that person has given consent. How? There should be clear guidelines in how consent is obtained and how that data is used. What will the penalties be for misuse of data? They should be severe or noone will be deterred from doing so. What comeback will people have if their data is misused?
6. Technology is not perfect and people who look similar could be accused of something they are innocent of. For example, identical twins, family members who look alike, although strangers could look alike. There should be back up and additional measures which people can utilise legitimately.
7. When someone passes away there should be a way of wiping all their data so it cannot be abused by someone for nefarious means.
8. There needs to be tight controls, especially regarding banks, in what can be collected for fraud prevention. Most people do not commit frauds and the draconian measures which banks are asking seem to far outstrip the benefits.
9. Employers should be tightly controlled in any use of biometrics in the workplace and the employees rights to not be constantly surveilled should be written in law. Otherwise workplaces will become very stressful. If people cannot relax at all that would be harmful to their productivity and mental health.
10. This Code needs to be put out to public debate in a transparent manner and discussed for at least a year.
11. The public cannot be expected to trust everyone who collects data to keep it safe and not abuse it. People should also be able to opt out and have a right to see all their data.

Nothing good will come out of this plan, dies no one have the foresight or ability to see other nations this occurs snd the detrimental effects ?
Not only an invasion and breach of privacy but out right dangerous in terms of storage, sharing and control as to who can utilise this and for what purposes?
Can we opt out?
Unfortunately mankind is too clever for their own good , too greedy for power and evil for control, this will be to the detriment of all so halt progress while we can.
Please listen to the people fir once, those who will be directly affected, fir should the tables turn, it won't end well.

Dear Comissioner,
I am writing because I am concerned with the use of biometrics and how it can be used too easily in harmful ways. Traditional methods of ID have been working so why do we need biometrics?
If biometrics is used how can one opt out?
I believe it is a technology we don't need and I don't want.
Thank you,

Sorry I ran out of time to read fully, but here are my responses to the major additional rules in the Code:

Should organisations assess whether using biometrics is proportionate, and be required to put in place privacy safeguards if they do use biometrics?

Absolutely yes. These assessments should also be made available to the public. Maybe a summary of why they are required and the privacy safeguards on their website, and on display on site. But able to request more detail.

Should people know about the use of biometrics beforehand, and should organisations have to provide additional information about the processing?

Again, absolutely yes. An example - Woolworths have a sign up by the door saying there is camera use at some checkouts. It should be mandatory to have a sign at each specific checkout where a camera is in use, advising customers. It should also say why it is necessary. In this example - weekly (or daily) reviews of the footage could isolate any footage of a customer stealing or abusing staff - the rest should then be destroyed.

Should there be limits on some uses of biometric information, like biometric emotion analysis and types of biometric categorisation?

Yes. Those two examples and probably others.

But the most important thing I want to say is:

It should be illegal to make availability to goods and services dependant on submitting to biometric analysis. That means a person could opt out of all biometric requests (they should all be requests not requirements) and still be able to access their bank account, shop in a specific store, access health or government services, travel freely, etc.

I would just like to say that I am not in favour of this change moving forward as I am very concerned about the privacy issues and safe guards.
The government gives itself powers to override any privacy concerns and if they have access to biometrics it would be worse.

We would like to register our objection to Biometric data collection. It doesn't matter how many rules and regulations are put in place, once that data has been stolen or corrupted it is the point of no return.

It seems that no organisation is guaranteed to be safe from their computer systems being hacked as demonstrated repeatedly over the years by global hacking of data from all sorts of systems including Governments, banks, multi million dollar companies etc etc.

There is exponential risk now with AI generating voice reproductions, image reproductions etc etc.

There is no "changing" our fingerprints or eyeballs as we can currently "change" our passwords and sign ins. Once biometric data is converted to digital for a computer to "read" it, that data can be compromised.

In summary, just because we can doesn't mean we should! If this Biometric industry is allowed to proliferate, there should absolutely be the option to opt out.

I am writing in regard to the Biometrics Processing Privacy Draft Code.

I am very concerned about the concept of biometric information being gathered from Individuals by anyone or any organization. Fundamentally to me it seems very un-human. This personal information is part of the sovereignty of the individual human being. I do not understand the hypothetical need to gather personal biometric information, it feels like a matter of - because we can, let's do it. There have been many things invented over time by humans, that have not made the world a better place. What is the purpose of biometric information other than gaining personal information from individuals which

could easily and potentially be used to their detriment by biased individuals or through data breaches and also create another data economy?

I believe the costs far out-weigh the benefits. I am concerned about who is going to hold the data? How is the data going to be safe? How is the data going to be protected? How is permission sought? Do we have an opt out? In a workplace what are the rights as an employee? How is the information going to be used? Is there auditing of biometric software? This draft code is not explicit in these areas. The people of New Zealand are not protected sufficiently.

Good afternoon, re the proposed new biometric processing privacy code.
Is this just more unwanted surveillance in the name of 'making things safer?'
There should be the option to opt out of biometrics being used to acquire information on people.
Will the person be told what information is being collected, the purpose for storing the information, who it will be shared with?
Is the government, police etc able to force this info to be turned over to them under certain circumstances?
Are alternatives to biometrics given to enable an Identity check?
This is a massive breach of privacy to acquire information without full disclosure.
Thank you for considering an alternative.

I welcome the opportunity to make submissions on the draft Biometric Processing Privacy Code of Practice ("the Code").

Please note I consent to my submission being published publicly, but not for my contact details or name to be released.

I believe this topic should have been advertised more to enable a national debate on it. It impacts every single person in NZ, and they should be able to comment on it. It's unfortunate that it wasn't advertised on that scale, where it was brought to the attention of everyone. It feels like this has been sneaked through, on the low-down. Only those in the industry or those who are keen-eyed who knew about it, and shared it with their networks, and encouraged submissions.

I believe the collection and use of biometric information causes a high level of risk to individuals and to society, which needs to be mitigated. A risk-based approach is needed for this issue, taking care not to under-regulate in a way that could leave individuals and communities open to harm.

I believe significant concerns remain around government surveillance, data misuse, and the potential for bias in biometric recognition systems.

Regarding the workplace - it makes me wonder what are the rights an employee has in terms of the collection of our data. That should be made crystal clear, have no ambiguity.
Is there even an option to "opt-out" in the workplace?? The right thing to do is to make it an "opt-in". Not everyone is going to want to have their data collected in the workplace. They will be happy with past processes/systems that worked perfectly fine until now. So it shouldn't automatically be assumed that everyone will want to adopt the new process. The regulations should include the responsibility being passed to the employer to seek individual's informed consent - not coercion - to have employee participation.

Dear Privacy commissioner,

I am deeply troubled by the privacy implications of the proposed Code's biometric data collection provisions.

The lack of clear consent and transparency surrounding its use, coupled with the potential for mass surveillance and discriminatory profiling, is unacceptable.

Biometric data, being permanent, presents unique and severe risks in the event of a breach.

I urge the Commissioner to implement stringent privacy protections, including mandatory opt-out mechanisms and explicit limitations on data usage, to address the inherent unreliability of emotion recognition and the dangers of data repurposing.

Moreover, the risks associated with large biometric databases, such as government overreach and corporate misuse, demand immediate attention.

[redacted]

[redacted]

Withheld to protect privacy, at submitters request.

[redacted]

Withheld to protect privacy, at submitters request.

I have not had the time or opportunity to study this issue in depth, but I did read through your proposed Code and feel concerned about it.

First of all, do we really need the collection of this type of personal biometric information, in the first place? (If so, why?)

I know that, for example, some banks (including in other countries) provide discounts or other benefits or, at the very least, greater "convenience", if one is willing to register one's voice- or finger-print, etc. This feels like an infringement of my rights.; it means that it is NOT a free choice, but rather, a loaded one. I would much rather put up with a little inconvenience rather than have my personal data on record. There is already too much data collection happening, as I understand it, e.g., via computers and smartphones, without my express consent - I feel that we do not need any more.

I feel concerned about security - especially considering the various large-scale data security breaches that have happened in recent years. Even if this data is ostensibly being collected for some relatively benign purpose, there could easily be a leak, and the information could well be used for other, more nefarious purposes.

I have one comment/feedback to provide.
Given that the definition can be technically complicated to apply, we think it may be useful to have a tool that Agencies could use to work through to determine whether the Code would apply.

I am commenting privately on the Draft Privacy Code.

Due to a variety of life-interferences, I have not been able to compose a calculated, written reply regarding the Code .

I thank you for linking the written assessment by Barrister Ben Keith, and I very much appreciated reading that assessment.

Nevertheless, my overall thought regarding the Draft Privacy Code is negative due to its various and incorporated complexities.

Therefore, I firmly believe that the New Zealand public would greatly benefit from an interactive discussion on the "Draft Privacy Code", either online, or at public venues, prior to the issuance by the Commissioner of a Biometric Processing Privacy Code of Practice.

Thank you very much for your attention to this.

I oppose the Biometric Processing Privacy Code proposal for the following reasons:

Insufficient public consultation. I only recently found out about this proposal and believe that most of the public in New Zealand are unaware of the Biometric Processing Privacy Code and its far-reaching implications for their personal privacy and security. There needs to be much wider education and consultation providing the pros and cons in an unbiased manner to ensure the public are properly informed of the issues and potential consequences.

It seems that the Government and Government departments have been pushing legislation and policy through in a rushed manner, including this proposal, to fit an agenda rather than engaging in full open and free debate with the public to ensure that any new legislation or policies really do benefit the best interests of New Zealanders and not foreign overseas global interests such as the United Nations, World Economic Forum, World Health Organization and many other NGOs. These organisations are funded by vested interests, as is the mainstream media organisations to promote a one-sided narrative. As has recently been highlighted by USAID funding of Reuters and the BBC and NZ Government funding of NZ media during the Covid 19 pandemic to promote a one-sided view regarding the response.

I value my privacy greatly and am very annoyed, to put it mildly, to recently have received a letter from NZ Inland Revenue Department informing me that they had shared my private data with, of all organisations, Meta/Facebook and Trade Me for goodness' sake without my permission!!

It is outrageous that a Government Department in NZ can be so lax securing private data of individuals. There are many documented cases of Government Departments and private corporations being hacked, including Biometric data, being stolen and sold on the dark web. Although your Privacy Code indicates the Biometric data will be kept safe and secure, I have lost all faith in the ability of NZ Government departments to do so.

There was huge Government over-reach during the Covid 19 response, using tactics of fear to coerce the public into complying with everything from masks, (proven not to work) social distancing (proven not to work) lockdowns (proven not to work) and experimental injections also proven definitely not safe and effective. There is much truth now being revealed about the amount of lies, deception and omission of truthful information provided to the New Zealand public, including suppression of alternative treatments and peer reviewed medical articles that contradict the Government and Ministry of Health narrative. I look forward to the second phase of the Covid 19 Phase 2 Inquiry being held that will be examining these matters further.

When it comes to privacy, safety and security, I have lost complete faith in the ability of the Government to ensure the welfare and wellbeing of New Zealanders, the NZ Government's track record is so far abysmal.

I chose to do my own research and inform myself, I therefore decided not to take the experimental injections being promoted as a safe and effective vaccine which they are definitely not, they are an experimental Gene Modification Therapy, and the public was gravely misled. I have no regrets choosing this course of action. However, I am greatly offended by statements of the then Prime Minister of New Zealand Jacinda Ardern who classed people like me as second-class citizens. And Chris Hipkins indicated that he would chase people up to ensure they complied with the vaccine role out. Many of my fellow Kiwis lost their jobs because they refused to comply with NZ Government or Employer mandates. I have personal family and friends whose health has been negatively impacted since taking these jabs forced on them, including some who have since passed away suddenly.

The Government over-reach that New Zealanders were subjected to smacked of East Germany Stasi tactics, had the Biometric Data been available to the level you are promoting, it would have made it much easier to track people down. Maybe that is the intent of this Biometric Processing Privacy Code? I probably sound cynical, I think not. I am expressing my personal feelings as to why this Biometric Processing Privacy Code must not proceed. The implication for the freedom, health and security of New Zealanders is too important to be rushed through.

I am against any compulsory biometrics data collection and storage by government, council, statutory body including the police and the health system.

- I am happy for people that wish to use such a system to do so.
- I do not trust the security of data systems already in place and there are repeated breaches occuring and have already occured in the Health dept, the police (breaches using photographs) and the IRD
- I am concerned that these systems lead to breaches of privacy, and facilitate excess power in the hands of beauracracies.
- The Government breached Human Rights during COVID 19 and misrepresented the science while promoting mistruths about safety and efficacy. Until we have a Government and its bodies that truly represent truth I will remain unwilling to give them more power (there are thousands of independent sources describing the dangers of the COVID 19 vaccines including countless dead and injured but our government ignores them).
- I have observed the police taking photographs of law abiding protestors and when challenged by the privacy commissioner they were very reluctant to abide by his decision. This is very concerning.

We have adequate security systems in place already and although we are throwing ourselves headlong into digital systems there are significant dangers and I would support a softly softly approach.

I observed the decline in student achievement in the classroom over the last 20 as evidenced by our appalling literacy and numeracy achievement results in ncea (and the decline in the international ratings). All the while being told as a teacher that we had a world class education system. I could see the introduction of electronic devices was not helping the problem despite the spin of successive governments, Ministry of Education and the teacher unions.

I have simply lost trust in officialdom and public and am unwilling to trust the statements of security and management by the public service. If your eyes were open to the opinions of many of the general public then they would tell you the same story, whether they had the willingness to respond to the endless submissions on digitization, currency, council operations, GMOs, COVID, lockdowns, traffic speed limits and many others.

I wish to retain physical cards, passports and pin privacy and reject digital identity and biometric data collection and storage by any authority.

Thank you for the opportunity to comment on the draft Biometric Processing Privacy Code of Practice. I have only recently been made aware of this consultation and I am concerned that the majority of New Zealanders are still in the dark about it and will miss the opportunity to give feedback. The majority of those I speak to do not even know what biometric data is, let alone how it is being collected and used in New Zealand at present!

The collection and use of biometric data and its associated technology threatens our current way of life and does not appear to align with the New Zealand Bill of Rights Act. As such, I question whether a code of practice of this type can be at all meaningful. Is this a voluntary code? If not, will it be enforced, how would this happen and what penalties exist for non compliance?

In my opinion, we need to take a step back and begin a very broad national conversation about the collection and use of biometric data before it becomes accepted as the norm. This conversation needs to cover all philosophical, ethical, psychological, cultural and health implications associated with the collection, use and storage of data. How do we give our consent? Is this informed or implied consent? If we do give consent, what exactly are we consenting to and for how long? Can consent be withdrawn? Who benefits from the information? Are services denied if we don't give our consent? Are we excluded from normal everyday activities that may disadvantage us if we refuse to consent? Will these technologies lead to discrimination of any kind? Where is biometric data stored? How safe is our data once collected and how long is it held for? What happens if data is stolen or used by bad actors? Are there physical costs associated with the collection, use and storage of biometric information? If so, who is paying for this? Has a cost/benefit analysis been done? What effect does the collection and use of biometric data have on health? Can we opt out?

I have already experienced being coerced to provide my biometric data and when I requested an alternative, I was belittled and discriminated against by staff who could not tell me what would happen to the data once collected. The business involved would not meet the standards outlined in this draft code of practice and may not be required to depending on the arrangements for enforcement. Is there any genuine justification for such a limitation on our freedoms and rights? Do we really want to continue on this path, and will a code of practice have any meaningful effect?

I recommend that your office call for a public duscussion/enquiry into the collection and use of biometric data before gazetting a code of practice. Just because we can, doesn't mean we have to! I believe that technology can be used ethically and for humanity's benefit but it can also be used to construct a living prison. I do not feel confident that the current draft code of practice is enough to safeguard us regarding this technology.

I would like to write in favour of limited data collecting and the preservation of privacy.

I think as little data as possible (ideally none) should be collected.
There are so many ways that data can be exploited. There are many reasons for this. Insurance companies abusing private information to hike insurance premiums, identity theft so criminals can buy things and leave us with the bill.
We can change a password, if our biometric data is being used instead, how can we change that?

A government department recently gave away data that people had to give to said department to a tech company, How much worse will it be if the data is biometric?

What if there is a hack? There have already been many hacks. Private companies? State intelligence agencies?

There is no particular gain for the people of New Zealand in having our biometric data collected and/or analysed.

There are so many downsides. The record is permanent. No one knows how things will shift in the future.

The Netherlands had a project to follow people "from the cradle to the grave". When a new power came in - namely the Nazis - this pre-existing data collection made it much harder for Jews to hide.

In France, the story was completely opposite. They had not done a census since the 1880's, did not collect data on religion for privacy reasons and were able to tell the Nazi's that they didn't know how many Jews there were, or where to find them.

Over 70% of the Jews in the Netherlands died. Around 25% of Jews in France died.

We cannot fully predict the ways in which data may be used and abused in the future. Technology in changing too quickly. But we can take note of how it is being abused today, and how it has been abused in the past.

Do not collect data for data's sake. Do not collect a permanent record heedless of the political winds shifting in the future. Do not pretend that the data is in any way invulnerable to exploitation and manipulation.

Please do not violate our basic privacy by making invasive biometrics a further part of New Zealand.

Dear Privacy Commissioner,
I am opposed to the Privacy Amendment Bill Act and changes it proposes to the Biometrics Processing and Privacy Code. No changes are needed here. New Zealand is not CCP-run China where there is no personal freedom or privacy.
Biometric ID is open to abuse of citizens via control, misuse and theft.
We already have ID systems that work satisfactorily but do not lead into a social credit system which the New Zealand public will not want and will resist. The NZ psyche and way of life would never be the enviable same, if we were all surveilled from the cradle to the grave.
Thank you for accepting feedback.

The Privacy Commissioner,

I am writing to share my concerns on the New Biometrics Processing Code.

I believe there are too many questions unanswered.

1) who will be holding this data?

2) There are and have been data breaches all ready. There is an inquiry pending where Statistics information has been used without consent
And possibly in a criminal way.

3) Once this information has been collected, there will never be an opportunity to own or keep private your information.

4) How is this information shared?

5) Can we opt out.

I do not believe the Biometric Processing is safe.
I do not believe we have a problem in New Zealand that requires such invasive measures.
I do not believe this will help New Zealand in any constructive way.

I believe a lot of this is unnecessary and is scary how we will be tracked and monitored.
2 factor authentication works well.
It's no use having face detection in places as the business themselves can't touch a person that may be a known shoplifter.

And I'm concerned that information stored will be used, as one of the clauses 7(b) override protection of information if it is deemed "necessary" - who decides this? And the ability to change this over successive governments.

There is also the implications of this information getting hacked (as this will happen one day) & what this will actually get used for? That could be devastating not only for the persons themselves but in the company's they work for (opening up access).

Thank you for seeking public feedback on this issue. A few years ago people were concerned about the mark of the beast in Revelation 13:16,17.
Today there is a bugeoning of surveillance technology enveloping all of us.

My first point is that the UN elevates the environment and animals to the same level as humans. We are becoming mere units in the production of our own demise; losing even our names on bank cards and 'branded' by cameras and electronic devices recording and classifying us. The gate is wide open and AI will strengthen and widen it.

We know that laws and regulations are meaningless without compliance so rules and laws for our compliance should not come from those who create them but truly independent administrators after wide public information and debate. NZ media has been silent.

Why do we need biometrics and who will benefit and at whose expense? Who will pay?

We must recognise that tech tools have been increasingly used to manipulate people and subliminally influence decisions, especially about 'health' in recent years. Could biometric identification using voice, fingerprints, eyes, gait or any other bodily feature be used to deny goods and services for non compliance? China comes to mind as an example.

We don't need multiple means of identification. Face to face interaction encourages honesty and minimises remote exploitation. Trustworthy people trust others.
However, currently there is a lot of unneccesary experimentation with new toys. This needs to be reined in by more stringent focus and no-one should be photographed or identified by any other means without their free consent.

In recent years sensitivity training and behavioural modification techniques have been repurposed in employment with only cursory awareness of the implications and consequences for employers and staff. Some people seem to be easily duped by the latest convenient devices to replace human labour.

Since children could be barred from sports and teachers from teaching by 'health' regulations what greater harm might biometric proliferation cause with compulsory curricula? Thought reform and brainwashing was abhorrent to us in the 1960s but we have short memories.

There could be strict limitations on type, location and purpose for biometric technology permission by a citezen panel before consent is given to use it. If granted, applicants should know that they will be monitored by citizen volunteers creating evidence to ensure limitation to the stated purpose in use. Please study the work of Dr Robert Epstein to implement this.

I believe collecting & storing biometric data is dangerously flawed & we should not go down this path.

Who is going to hold this data? Who is going to have access to it?
Typical feature creep would suggest by no great leap of imagination, it being shared to banks, health & insurance companies - more points of potential data leak &, or attack by bad actors. & also as you also point out "data must not leave NZ unless it's to somewhere that has similar laws for handling data" - a clear admission of reserving intention to later share data that should only be held for the purpose it was collected, illegally with other countries. We have seen
similar ill informed policy happen with the "progress of tech", where data leaks & attacks have happened countless times in the past & continue to do so today. This would be inviting a total catastrophe upon the nation & is hence not in anyone's best interests.
We already see data breaches that have led to identity theft, if you have a data breach in a biometrics system, the potential damage to an individual is unlimitless. & will be a damage that cannot be undone.

Within your own documation you set out some reasonably sounding policy, only to later negate said points with caveats with more holes than a colander: Once more "data must not leave NZ unless it's to somewhere that has similar laws for handling data" - a disturbingly nebulous definition at best - & as already pointed out, the data can only be legally used for the intention it was collected - not to be shared with other people & certainly not entities in other countries, rule 10.5 from the "BIOMETRIC PROCESSING PRIVACY CODE DRAFT" defines limitations of use only for 10.7 to pepper the inferred words of reassurances also with holes. The whole documentation is intentionally misleading & verbose, I can only think for the purpose of misleading people & I imagine

We have already seen nefarious government policy that collected data during Covid be reused for other purposes. One of the basics of data management is that it should only be used for the purpose it was collected.

All thoughts & feedback most gratefully appreciated

I oppose the implementation of the Biometric Processing Privacy Code for the following reasons:
The code will set the path for the use of biometric data into the future. It is of immense importance for the safety and well-being of New Zealanders.
The initial phase of the consultation was for barely a month and the second phase ran through the main holiday period. The announcements regarding the draft biometric code have been on the Office of the Privacy Commissioner's own website, rather than on Parliament's website, where nationally important consultation documents are typically posted. New Zealanders who were not already aware that the consultation process was taking place would not have been regularly checking for developments of major national importance there. There has been little mention of the entire issue in the nation's media. Not enough has been done to ensure the general public is aware of the consultation process and the issues.
Therefore, the whole consultation process has been inadequate and this needs to be addressed before pressing on with the process. This is too important for our future to have so few New Zealanders aware of what is happening.

The gathering of biometric information is already being abused in New Zealand today. Some government departments are already monitoring, analysing and assessing computer keystrokes in communications from members of the public. "Decisions" are then made on what so much as a pause in typing a sentence means in terms of the motivation of the writer. When in fact the pause may simply mean that the writer had to use the bathroom or answer the phone. The vast majority of New Zealand citizens are completely unaware that this is happening with regard to their communications. This should never happen. The "judges" at the Dept. are not able to read people's minds although, highly inappropriately, they act as if they know people's motives without any doubt. This is just one example of how this type of information can be misused by those who have acquired the power to "judge" and in many cases "sentence" others wrongly.
The inadequacy of those who are holding the public's biometric data has already been shown through multiple leaks and hacks. I for one have no confidence that increased power over exponentially increased biometric data will be handled any better.
The stakes for individual New Zealanders are extremely high, and there appear to be no real safety nets when things go wrong, just a shrug and "we acted within the law".
Right to privacy is a crucial tenet of a free and democratic society; and that is what New Zealanders want, not an Orwellian nightmare.

I wish to oppose the Privacy Commissioner's new Biometric Processing Privacy Code because biometrics are creeping into our workplaces, airports and public spaces without the public being informed and with the potential for being used unethically.

Surveillance and psychological/digital manipulation with A.I. also being thrown at people appears to be a mitigated war on privacy and security.

Why does New Zealand need this change in biometric privacy?

Facial recognition, gait recognition and digital identification can be incorrect and identify the wrong person without any way of countering it once targeted.

Who is going to be in charge of this information?

Where is this information to be stored?

How secure will this information be?

For example, New Zealand sent the results of the Covid-19 Rat Tests to Israel who then were caught selling the data, the New Zealand Department of Inland Revenue has recently leaked thousands of New Zealanders data to do with Facebook, including my own daughter's, and do not know where it has gone as well as the myriad of cyber attacks.

With any emerging technologies, MONITORING has to be a part of it so at least the public of New Zealand knows what is happening and have transparency.

We can not trust the government to be in charge of monitoring due to a conflict of interest.

The internet was supposed to connect people, instead this is proposing to divide us and manipulate us.

We oppose the collection of biometric information on the grounds that it will violate our privacy and human rights. It would make it easier for individuals to be targeted by unscrupulous political leaders as witnessed during the COVID mandates.

It would lead to digital identity and social scoring as seen in China, which is another violation of New Zealanders' human rights.
All the safety measures proposed can be violated.

I'm writing to express my concerns about the biometrics privacy. The current draft code is not very clear at all.
I have a lot of concerns and the more I read the more concerned I become.

Why do you need to do this? It was only a short time ago that everyone (including the New Zealand government) was condemning the Chinese government over there overstep and abuse of surveillance (and unfortunately it looks to me like the New Zealand government has forgotten all to soon and are trying to do the same here). And what benefit has it had in China? The answer would be a lot of international condemnation against the abuse of privacy and human rights! Why would New Zealand want to follow this?

In the code, if it wasn't to be rule as unjust and abuse of power, is there a way that people can opt out? What about people who don't like how they look? It's already dangerous when I drive as I can't stand seeing cameras and try to hind from the two in the road (if I go that way). This isn't because I'm afraid or have broken a law or anything but I just don't like being on camera (especially when I don't know who's going to be looking at it or what it's going to be used for). What about people who've been abused? (I mean, you could say, that's way I'm afraid of cameras now due to how I was treated in regards to some photos of me when I was younger).

This code is very lax and I would not feel safe living in New Zealand if it goes through like this. Who would be able to see my photos etc? Who would you share them with and what would be the laws around what they could do with them? What does "similar laws" mean in terms of countries you may share them with? (This is about as vague as a law/code can be in my opinion. Anyone in law can interpret it as they want to fit what they want. And that is not safe!)

I seriously OBJECT to a Biometric bill/ legislation of any kind - this is totally unnecessary and raises privacy concerns as hackers can get into any system and take anyone's data - these systems are not SAFE. Its a further method of control and is Orwellian in its nature, and against our rights to privacy.

Anyone implementing this is a controlling authoritarian state and it should be thrown in the bin.

I am writing re the proposed code. I am very perplexed about this widening use of biometrics.

Having looked at your guide, I am left wondering what the purpose of this code is. It seems to be a solution without a problem! As we know, there are many breaches of data privacy daily. This expanded use of biometrics and collecting people's data only multiplies the risk of further breaches. Once a breach has occurred, there is no facility to recover the data lost.

I believe we have enough systems in place to check identity already, so this proposal is superfluous. I also worry about usage of data collected now to be used for unknown purposes in future.

Additionally, in your guide, it states that data can be used for public health or safety reasons. This is subjective and contradicts the Human Bill of Rights for privacy. Please answer the following questions:

- Please clarify what you mean by public health and safety.
- How is the data going to be used?
- How are people's permission going to be collected?

- How can someone opt out of having their data collected?

Submission to Te Mana Mātāpono Matatapu / Privacy Commissioner regarding the draft Biometric Processing Privacy Code of Practice

Monday 17 February

Kia ora,

Thank you for the opportunity to submit on the draft Biometric Processing Privacy Code of Practice.

We are at an important crossroads in terms of the nexus of machine learning, artificial intelligence, facial recognition and other technologies which can mine the already ubiquitous and cheap surveillance technology for biometric data.

All the massive amounts of other data which normal citizens are essentially forced to give up — to do anything via The Internet, purchasing things via a credit card, interacting with friends, family and community via social media, and other funnels which skim information about us so it can be monetised — means the companies who store this data have creepily good datasets including images, videos, and more about folks just going about their everyday lives.

These guidelines go some way to limiting the collection, storage, and use of biometric data — some of the most personal information about a person an organisation can collect. I generally support the Code of Practice as it stands but think it can be clarified and strengthened in order to further protect New Zealanders privacy.

Regarding the three main questions you are seeking feedback on, my answers are as follows.

Should organisations assess whether using biometrics is proportionate, and be required to put in place privacy safeguards if they do use biometrics?
Yes on both counts. There should be a defined process by which organisations need to assess the collection of biometrics before they start collecting. This document should also be required to be made public by the organisation.
There should be auditing of their plan for implementation of biometric collection and if the organisation is doing everything it can to comply with the code and relevant laws. There should be significant penalties if organisations are found to not be adhering to their own processes, the code, and other relevant rules and laws. When an organisation decides to collect biometric information, all staff who will be required to engage in its collection should be given comprehensive privacy training. The platforms which organisations use

to capture and retain biometric information should have the highest level of privacy safeguards built into them, including tools which monitor potential misuse of the information.

Should people know about the use of biometrics beforehand, and should organisations have to provide additional information about the processing?
Yes on both counts. Any organisation which collects, stores, processes, or helps other organisations use biometric information should have to visibly and clearly communicate with the people whose biometric information they are collecting and storing. There needs to be clear guidelines about what level of communication is needed. A small sign, a section on a website, or a line in a lengthy Terms of Service agreement is not good enough. The collection of biometric data, and the ramifications of an organisation capturing that information and storing it, should have to be made abundantly clear to people and people

should have to actively agree to its collection. As should the pathways to ensuring an organisation does not capture a person's biometric information — or deletes it if requested. Asking for your biometric data to not be recorded should be an option, and asking for it to be deleted should be easy. Once again, there should be significant penalties if organisations are found to be collecting biometrics without the enthusiastic knowledge of the people whose information is being collected. Organisations which collect biometric data should also have to make it clear exactly how that data will be processed, who is processing it, and what technology is being used to do the processing.

Should there be limits on some uses of biometric information, like biometric emotion analysis and types of biometric categorisation? Yes. While there are some specific instances where these might be useful — for example the recent story about how AI is being used to save lives in swimming pools — for the most part, further analysis of people should not be able to be used unless a very high bar has been cleared. Organisations which can do this should have to adhere to the highest levels of privacy and data security to ensure the biometrics are not misused, hacked, or used to target people.

Review of the draft code

Overview

•I generally support the draft Biometric Processing Privacy Code of Practice.

•There are instances where rules need to be further clarified or additional resources developed to help organisations navigate these rules.
•Biometric data, its collection, storage, processing, and use should be treated as some of the most confidential information an organisation can collect about a person.

•Given the state of technology around biometric information and the rapidly encroachment of surveillance and large data sets of crowdsourced "intelligence" being used to combat theft from stores, these rules need to recognise the companies operating in this space will be very good at sticking to the letter or the rules, but not necessarily the intent.
•Given any video or image of a person can now — through machine learning, facial recognition, and/or artificial intelligence — be easily turned into biometric data, and surveillance technology is cheap and ubiquitous, the rules need to treat any image/video gathering as the collection of biometric data.
•Needs further clarification of who is able to hold biometric data. For example, if a shop uses a platform to collect a database of folks who are suspected of shoplifting, do they have to self host the data or is it okay for the platform to host it? The privacy problem really comes into play when a single store's database is connected with other stores. This allows staff with access to the platform, the police, or potentially the platform itself to essentially track people in a way that is deeply creepy.

Detailed feedback on the rules

Rule 1

Needs to be clearer about when it is okay to collect biometrics. There needs to be specific guidance about what "necessary" means. Can an organisation just

say it is necessary? An example of this in action might be a retail store, ostensibly the owner may claim collecting biometrics are necessary to prevent shoplifting, but there is no clear pathway to explain how this will reduce theft and there are other interventions which might better be able to prevent theft.

Rule one needs to be supported by a mechanism, framework, process, or toolkit to allow organisations which want to start collecting biometric information to determine whether it is necessary, no

alternatives exist, and is proportionate.Without a clear framework there isn't really anything to stop an organisation saying they did consider these things.

This framework should be provided by the Office of the Privacy Commissioner and not from a third party or the product which is the organisation's technology for capturing biometrics. Organisations should have to make this document public before they start using biometrics.

Rules 2 and 3

I agree all biometric information needs to be collected directly from the individual.

However, there should be active consent needed by the individual.

A small sign or one section buried in a lengthy End User License Agreement or Terms and Conditions in an app or website should simply not be good enough to satisfy this rule.

Rule 3 should also include a section about how the data is stored and what metadata can be extracted. Some services claim they don't use facial recognition technology, they just go off metadata and with enough metadata about a person it is also easy to identify them.

In some instances, CCTV footage and other video and images are being collected and then loaded into platforms which then convert images to data/ metadata about a person, and can be tied to profiles across stores, it is important this rule reflects that any surveillance in a store could be used to create biometric data.

Rule 4

Agree with this rule and echo the feedback for rules 2 and 3: there needs to be active consent for biometrics being collected.

Rule 5

Needs further clarification regarding who is able to hold biometric data. For example, if a shop uses a third party platform to collate a database of folks who are suspected of shoplifting, do they have to self host the data or is it

okay for the platform to host it? If they're just suspected of shoplifting, is that bar high enough to warrant disclosure?

The privacy problem really comes into play when a single store's database is connected with other stores' databases. This allows staff with access to the platform, the police, or potentially the platform itself to essentially track people in a way that is deeply creepy.

Rule 6

Needs to be strengthened to ensure accessing your own biometric information is simple, easy and accessible.

Rule 7

Needs to be strengthened to ensure correcting your own biometric information is simple, easy and accessible.

Rule 8

This needs to be strengthened to reflect machine learning, facial recognition, and AI image identification — alongside surveillance technology — are now cheap, ubiquitous, and automated.

There are many concerns about these technologies misidentifying people.

Rule 8 should better reflect the need for humans to actually be the ones inputting data and information. This is especially important because we know there are platforms which disclose photos, videos, descriptions and other biometric data — linked to other identifying data — directly to New Zealand Police.

Rule 9

Needs to set a firmer length of time and circumstances for which biometrics can be held. It is likely organisations will argue they should be able to hold this data indefinitely, especially when it comes to the platforms being used in retail settings.

Rule 10

Broadly agree with this rule. Any organisation which collects and uses biometric data should have the highest level of scrutiny placed on its use. The use of biometric information should be limited to clearly defined instances and follow clearly defined protocols, which ensure the privacy of the person and the security of the data.

Rule 11

Needs to be made clearer in terms of when it is okay for an organisation to disclose biometric information. For example, some platforms currently allow retail staff to add images, video, and descriptions of people who they suspect

of shoplifting to a database. The New Zealand Police have access to this database of folks who might just be using a tote bag in a store.

In this example, Rule 11 should also require the store to inform the person they have been added to the database and it is now accessible to the police and potentially other stores.

Rule 12

Given many of the providers of machine learning/AI/etc technologies are not based in New Zealand and the structure of cloud servers means biometric data might be stored in data centres outside of New Zealand, and thus accessible to foreign persons or entities, this rule needs to be significantly strengthened.

Biometric data about New Zealanders should be stored securely in New Zealand.

Organisations should only be able to disclose biometrics to a foreign person or entity if there is a legal obligation to do so.

Rule 13

This is good and will limit how folks can be tracked across different instances of biometric information gathering. Once again, there needs to be some monitoring of, enforcement of, and penalty for breaking this rule.

Conclusion

We have allowed an industry of private surveillance and intelligence gathering to skirt privacy laws for far too long, amassing a significant amount of information and data on New Zealanders. It's creepy, it is disconcerting.

Recent stories about one such platform, and the response to them, show that while these companies might be complying to existing — and potentially out of date — laws and rules, they are perhaps not being particularly ethical about their practices. It is dubious as to whether these companies have the privacy or safety of New Zealanders at heart, and most New Zealanders do not know or understand the extent to which their biometrics are being collected, stored, and potentially used.

As we have seen, time and time again over the past 25 years, it's not a matter of if, but when a data breach occurs. These rules need to make it clear biometric data needs to be stored securely. Given some estimates put the uptake of one particular platform which allows organisations to upload

biometric data at roughly 90% of retail stores in New Zealand a data breach of their systems could have massive impacts for almost all New Zealanders.

A Code will go a long way to curbing the creepiness of the rampant collection of very personal information about people. This draft code, and privacy law in New Zealand, can and should be strengthened to ensure privacy is the default setting when it comes to the collection of biometrics. It will also help increase public trust for those organisations which do collect and use biometrics lawfully and ethically.

Thank you again for taking the time to consider this submission. I am happy to speak further about these issues and concerns I have raised here. I look forward to seeing the next iteration of this code soon.

Kind regards,

[redacted]

1.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, I agree the Code applies to any organisation, public or private, using biometric processing.

2.Do you agree with the exclusion for health agencies?

Possibly, but were FRT used in the example provided (in the emergency waiting room) on employee or non-health related, then they definitely need to adhere to the Code. I don't like the idea of it being used in places like emergency waiting rooms where we have no choice in the matter where it is necessary to be there.

The special provisions afforded to intelligence agencies, NZ Police, Border control or other ought to have clear consequences for violation of fair use. We have already seen NZ Police use FRT where the Police Commissioner wasn't aware of it, and trial other invasive technology without public notification (E.g. Pimeyes). I want clear accountability and real consequences for overreach. Personally, I think it's highly unfair to be living under a surveillance state where public organisations access and use invasive tech where too often, health and safety, is used as an excuse for further restrictions on our freedom.

Concerning as well is the Government's Social Wellbeing Agency which aims to use massive amounts of our data for 'targeted' social investment. This agency better not use FRT or predictive analytics without the utmost transparency and public scrutiny.

Furthermore, if ordinary people are wearing META sunglasses enabled with FRT, why do they not have to comply with the CODE? If I see someone filming me with those glasses on I will snatch them off their face, throw them to the ground, and smash them with my foot. Most people do not like being filmed in public without their consent. In the above example, my response would be adequate given the highly offensive and intrusive nature of those types of sunglasses.

3.Do you have any comments or questions about the interaction between the Code and other laws with biometrics provisions?

I haven't read other laws with biometric provisions so no comment. Regarding the HIPC, I totally agree it should be revisited if insurance companies are itching to use FRT. Thanks to the insurance industry the use of CCTV is now rampant. Awakening to the tech creep happening in our everyday lives from CCTV, ANPR, and FRT has increased my anxiety tenfold. Every time I go out now, I am looking for where the cameras are and wishing I could destroy all of them.

4.Do you have any feedback on the guidance on who the Code applies to? (See pages 11-13)

5.Do you agree that the rules in the Code should apply immediately to any organisation that starts using biometrics after the Code comes into force?

Yes, for too long now New Zealanders have been left in the dark, more than a third do not understand the tech, and over half of us are concerned about our privacy rights. The Code should apply immediately to any organisation that starts using biometrics.

6.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?

No, that is far too long a period. FSNI has been using FRT since as early as 2018 (conducted covertly at that time). Their activities and systems contributed to harm then and are actively contributing to harm now. Furthermore, FSNI is not getting informed consent and that's wrong. The commencement period for the Code must be immediate.

7.Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?

Yes, they are clear and understandable

8.Do you agree with the definition of biometric processing and related definitions (biometric verification, identification and categorisation)?

Yes

9.Do you agree with the information types excluded from biometric information (biological, genetic, brain and nervous system material)?

How does the Government's desire for roadside random drug screening fit in with the biological component of the CODE? Taking a sample of our DNA via a swab of our inner cheek (outside of a health context) appears relevant to regulate as it could be used in biometric processing without our knowledge.

10.Do you agree with the processes excluded from biometric categorisation and the way they are described (readily apparent expression and analytical process integrated in a commercial service)?

I agree with the exclusion for a commercial service but I'm not sure about readily apparent expressions. Detecting overt behaviours does create a risk they will be used to infer deeper psychological states.

11.Do you have any feedback on the guidance on what the Code applies to? (See pages 5-13)

I am relieved that our concerns are being taken seriously and there is work underway by your office to protect our privacy (and human rights) against increasing surveillance. I wish Peter Thiel was never granted NZ citizenship and that his business, Palantir, restricted its facial recognition technology product to warfare use only. I wish the Labour minister at the time (Megan Woods) didn't sign off on the master agreement between DXC Technologies and DIA which allowed public and private organisations to bypass the public tendering system. In doing that, the doors to using invasive tech were thrown wide open resulting in the harm and misidentification of everyday New Zealanders just trying to buy their groceries. I wonder greatly why the use of surveillance tools rose so quickly during and after the pandemic.

12.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, assessments of effectiveness and checking for alternatives are a necessity for any organisation using biometrics. For example, there were a number of KNOWN alternatives to use to protect against theft and bad behaviour at our essential stores but Chris Quin, CEO of FSNI let his ego cloud his judgement and trailed invasive technology with KNOWN bias and at settings that invited preventable harm and racialised discrimination. He was warned but went ahead with the trial, and now they are claiming success but misleading the general public pointing to 3rd party independent assessors which were not independent at all. His general counsel, Julian Benefield, points to a customer survey showing 9/10 customers are OK with the trial but we all know the way questionnaires are designed can influence the answers and when he was asked to share the survey, he did not. What are they hiding? Certainly, the 'results' of their trial have been skewed as well and what would be good to know is the ethnicity of all those misidentified,

13.Do you agree that organisations must consider whether the processing is proportionate to the impacts?

Definitely, in the case of FSNI their trial fails the proportionality assessment on 5 of 6 points. It is astounding that after warnings from the Privacy Commissioner, Dr. Karaitiana Tuira, Consumer.org, everyday New Zealanders like myself and many others, they still went ahead with it and unsurprisingly caused preventable harm and racialised discrimination of a Māori woman. Not to mention all the other 9 misidentifications (that we know about).

So proportionally, their trial causes more harm than good. Their claims are not to be trusted and one questions why they didn't use KNOWN alternatives instead of reaching for invasive tech.

Imagine the positive effect it would have if they paid all their employees and contractors living or thriving wages instead of opting to invest money in surveillance tools used by Autocrats. Shameful!!!

Do you agree with the factors that go into this assessment (degree of privacy risk, the benefits, any cultural impacts on Māori)?

Not entirely. While I agree we definitely need to address the impacts on Maori and other dark skinned people since we know these groups are treated differently by this technology, I want to recognise the impacts on non-Maori, too. We must address the heightened anxieties people are experiencing because of witnessing increasing use of invasive surveillance. We see in news articles about surveillance in the workplace contributing to rising levels of anxieties, the same is true concerning its use in our essential services and where public life convenes.

14.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?

Of course safeguards must be required which is why I have raised a claim in the Human Rights Review Tribunal naming FSNI as Defendant. Their so-called 15 month consultation period resulted in them adopting settings which invited the preventable harm and racialised discrimination of a Maori woman. Their weak safeguards failed her and the other mis-identified shoppers.

Even if FSNI implements robust safeguards to lower the risks, the collection is not proportionate. They have already lost our trust. I want FRT out of our essential services and where public life convenes. It is such a gross overreach.

Safeguard examples ought to be listed in the Code. For example, setting an alert threshold at 99% is a start. FSNI had theirs at 87 or 90 and only after causing preventable harm did they raise it to 93. Still too low!!! And, why even after the trail has ended are they still collecting, recording and storing our biometric data. So they can grow their data set sizes to say, see it's diverse and balanced so we should be able to keep using it. GROSS. They are not getting informed consent and they don't care because they want to keep using their tech toys.

Chris Quin may think he has a clear purpose for using FRT (to reduce theft and bad behaviour) but there are KNOWN LESS INVASIVE alternatives but he and the board ignored them.

15.Do you agree with the new trial provision? 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?

I see more preventable harm to be caused with the industry demand for this technology and a trial provision will add to it, no doubt. CEOs and board members wanted a quick fix for rising theft and bad behaviour ignoring the context for it (Pandemic/cost of living crisis). Too often, a grab is made for tech to solve social problems but that's lazy. So, yes, I see risks for a provision to trial the tech. Which is why there MUST be a substantial monetary award when preventable

harm is caused. Which is why there MUST be informed consent, individually requested, before our biometric data is collected.

Of course, all the rules should apply while a trial is being conducted. Why should innocent people pay the price for an organisation's poor planning and implementation?

Why are we leaving it up to the organisation to assess the effectiveness? FSNI is already misleading the public about their trial. And, there should be no extensions. Period. If six months wasn't long enough, too bad.

16.Do you have any feedback on the guidance for rule 1? (See pages 21-63). In particular, do you have feedback on our example use cases? We envisage developing a decision tree for rule 1, would this be useful? Do you have any feedback on the section on the cultural impacts on Māori? For Māori individuals or organisations, are there any other impacts we should discuss?

Sorry, but I can't find those pages or example use cases. However I imagine a decision tree would be useful. I'm not Maori and therefore can not speak to the cultural impacts but I can speak to the impact on FRT on dark skinned people, particularly women. I was alarmed when I read about FSNI'S trail in Feb. 2024 and I felt livid when I read less than two months later about the preventable harm and racialised discrimination it caused a Maori woman doing her shopping on her 47th birthday. So. very. wrong.

Questions about Rule 2

17.Do agree with the modification to the rule 2 exception to make it stricter?

Yes, let's make it stricter.

18.Do you have any feedback on the guidance for rule 2? (See pages 63-74)

Questions about the notification obligations in rule 3

19.Do you agree with the new minimum notification rule, that requires, at minimum, clear and conspicuous notice of a few key matters?

The minimum notification rule is too weak. I have already shared the first hand knowledge I gathered while protesting in front of my local Pak N Save. People DID NOT KNOW they were providing consent for their faceprints to be recorded, collected and stored. The posters on the windows are WHOLLY INADEQUATE.

Here are some ideas from Co-Pilot

Digital Signage: Use screens and digital displays throughout the store to inform customers about the use of facial recognition and how their data will be used.
Mobile Apps: If your store has a mobile app, include a section where users can read about the technology and provide their consent within the app.
Website Notification: Post detailed information and consent forms on your store's website where customers can review and provide their consent online.
Email Communication: Send an email to your customers explaining the use of facial recognition technology and include a link to a consent form.
In-Person Explanation: Train staff to explain the technology and obtain consent at the point of entry or checkout, ensuring that customers understand what they are consenting to.
QR Codes: Place QR codes around the store that customers can scan to access information about facial recognition and consent forms.

20.Do you agree with the additional matters for notification? Do they require organisations to provide useful information? Are they workable?

Absolutely I agree an organisation must share their proportionality assessment. It is their responsibility to demonstrate WHY they are using invasive surveillance and HOW they came to reason it was the right choice to make. Along with the additional matters outlined in the statutory consultation draft.

21.Do you agree with the removal of two notification exceptions?

I do not agree with the exceptions for statistical or research. I can see our Social Wellbeing Agency taking advantage of this one.

Also, where the information will be used in a form where the person wouldn't be identified is dubious as we've seen how IRD thought our data was anonymised and it turns out that wasn't true. Selling that data to Fakebook is a disgusting breach of our privacy especially considering some of us have never signed up to Fakebook.

22.Do you have any feedback on our rule 3 guidance? (See pages 74-87)

Posters on windows are so last century and are absolutely NOT gaining informed consent. The Maori woman harmed by FSNI did not even know the store was trialing FRT and many of the shoppers I spoke with did not know either. That is NOT ok. Digital signage and informed consent must be an absolute minimum - no more posters on store windows!!!!

23.Do you agree that an organisation should have to tell the individual what form of biometric information they hold about them?

Yes, of course an organisation should have to tell the individual what form of biometric information they hold about them.

24.Do you have any feedback on our rule 6 guidance? (See pages 87-92)

27.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 absolutely Do you agree with the exception where the individual has given their express consent? Let's use the word, informed, rather than express. Do you anticipate risks or beneficial uses? Yes I anticipate risks just like when I read in Feb. 2024 that FSNI were conducting a trial I wrote to them to warn them of the bias inherent in FRT and less than two months later my concerns were validated.

28.Do you agree there should be limits around using biometric emotion recognition? Are you aware of high-risk or beneficial use cases?

There should be more than limits, it should be restricted.

29.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?

There should be more than limits, organisations should be restricted from using biometrics to categorise people into certain sensitive groups. The concerns outweigh the benefits.

30.Do you think any other uses of biometric information should be restricted?

Here are some:

Surveillance and Monitoring:
●Mass Surveillance: Restricting the use of facial recognition and other biometric technologies for mass surveillance by governments or private entities without clear legal guidelines and oversight.

Law Enforcement:
●Predictive Policing: Limiting the use of biometrics in predictive policing, which can lead to biased and discriminatory practices.
●Unauthorized Access: Preventing law enforcement from accessing biometric data without proper legal authorization or oversight.

Employment:
●Employee Monitoring: Restricting the continuous monitoring of employees' biometric data to avoid privacy violations and potential discrimination.
●Hiring Practices: Limiting the use of biometrics in hiring processes to prevent biased decision-making.

Consumer Tracking:
●Behavioral Profiling: Restricting the use of biometrics for tracking and profiling consumers' behavior without explicit consent.
●Targeted Advertising: Limiting the use of biometric data for personalized advertising without the users' informed consent.

Healthcare:
●Insurance Discrimination: Preventing insurance companies from using biometric data to discriminate against individuals based on health conditions or genetic information.
●Unauthorized Sharing: Restricting the sharing of biometric health data without patients' explicit consent.

General Privacy:
●Data Sharing: Limiting the sharing of biometric data between organizations without the individual's consent.
●Retention Periods: Imposing strict guidelines on how long biometric data can be retained and ensuring it is securely deleted when no longer needed.

31.Do you agree with the general exceptions to the limits (the exceptions for accessibility, preventing a serious threat to health or safety, and research purposes)? Do you think there needs to be other exceptions, and if so, why?

No, I don’t agree as I think these could be used as a loophole UNLESS there is clear oversight. Again, I think our social wellbeing agency will want this for research purposes and I don’t think that’s ok as it would depend on who sits on the ethics oversight panel. And, Define a serious threat. Words like serious and health and safety are too broad and often used as loopholes.

32.Do you agree with the exceptions provided for using biometric information for different purposes in rule 10(9)? Do you think there should be more exceptions or fewer?

I disagree with removing age estimation, it should remain in the CODE.

33.Do you have any feedback on our rule 10(5) guidance? (See pages 93-98)

Questions about Rule 12 34.Do you agree that organisations should ensure that adequate safeguards, reflecting those in the biometrics Code, are in place if sending biometric information overseas?

We're seeing in the news that talks are continuing about whether New Zealand will share criminal offending with our Five Eyes partners (global surveillance is now in our essential

services - so sad). I think if they decide to share that they will most likely share biometric info. Overseas, too. It's a slippery slope. We already know the USA has very few protections on the use of biometric data. They will use surveillance against migrants, illegal or not, pregnant women (fuck Trump and the SCOTUS), and everyday citizens who are tracked everywhere they go. We need less tracking and more trusting.

35.Do you agree with the intent of the reference to biometric features and templates in rule 13? Does this change help provide clarity on how rule 13 would apply?

Yes, I agree.

36.Do you have any other questions, comments or suggestions about the Code or guidance?

I have submitted an OIA to DIA to ask for a list of all private and public organisations that are already using FRT. I would like it published online, updated and tracked. Does the OPC support this action?

When will NZ conduct a public perception survey of FRT like Australia did in May 2024? Results of it showed people did not want FRT in their essential services. It showed most people don't understand biometric information/processing/categorisation etc.

Can the CODE be in place by mid 2025 as predicted?

What does the OPC consider fair compensation when biometric processing results in a breach of privacy, preventable harm or racialised discrimination?

Submission in personal capacity / individual From [redacted]
Date: Friday 14 March 2025
To: The Office of the Privacy Commissioner, Biometrics Privacy Consultation Team
Consultation submission
- Biometric Processing Privacy Code (Consultation Draft – December 2024)
- Biometric Processing Privacy Code – draft guide (December 2024)
- Biometric Processing Privacy Code: consultation paper (December 2024)

1.I welcome an opportunity to discuss with your team (oral meeting). To provide an opportunity to answer any questions you may have. Whether for clarity on my submission, or anything else.

General

2.I support the Privacy Commissioner's intent that biometric processing needs better privacy requirements.

3.I generally support the Privacy Commissioner consultations on biometric processing.

4.I am concerned the consultation rounds have not been extensive enough. Nor was I aware of them until recently.

5.I am concerned that much wider consultation is needed in this area, as the approach is profound.

I support privacy risk
6.I support privacy risk in the Code section 3 (2).
Opinion: Organisations under appreciate privacy risks and biometric processing privacy risks

7.In my opinion, I believe organisations have a variable to poor understanding or effectiveness with the Privacy Act for handling personal information (including non-biometric personal information).

8.In my opinion, I believe organisations have and will have a variable to poor understanding or effectiveness for handling biometric privacy. Primarily due to under appreciating or poor understanding of the limitations of the technologies, the technology and systems risks, and human factors / biases.

9.In my opinion, I believe organisations will have a variable to poor effectiveness with the Biometric Processing Privacy Code (in principle). Given the poor attitudes towards biometric risks and appreciating the Code. In principle, I believe this will limits effectiveness. Regardless that the Code guide and other guidance may potentially educate and raise levels of awareness, I believe that ultimately it will not be enough.

10.In my opinion, the factors limiting effectiveness are ultimately based on the organisations; regardless of the Code.

11.I am also sensitive to the Code itself. In general I am partly supportive, and partly opposing. Yes it is important to get it right.

Non-biometric alternatives. I prefer must offer alternatives
12.I believe it is important that non-biometric processing alternatives must always be an option and notified. I oppose biometric processing without alternatives; or coercion that (must) use biometrics.

13.As part of Rule 3, I oppose Rule 3(1)(c) "whether there is any alternative option to biometric processing that is available to; ..."

14.I would support adding to the Code that
a.alternative options to biometric processing must be available;
b.and consequentially revise Rule 3(1)(c) wording for somelike like "advising of alternative options to biometric processing".

I partially support Biometric Verification
15.I partly support the intent of Biometric Verification. As this concerns the individual's verification. Though even that comes with many privacy risks and side effects, to manage under the Code.

16.I partly oppose, may need much tighter controls also for associate behaviour biometrics (including opt-in and alternatives).

17.I may conditionally support Biometric Verification constrained to the user (depending how implemented). That is, if only used for Biometric Verification (1:1) despite it being a 1:many biometric system. Conditional on user's opt-in, and protecting the larger system. Unfortunately, the larger system is more vulnerable (or all users privacy may be potentially vulnerable). In practice, privacy risks for that 1:many system being breached. I partly oppose as part of a 1:many backend, given the increased magnitude of potential privacy risks including scope creep and security breaches.
I oppose Biometric Identification (one-to-many)

18.I am generally opposed to Biometric Identification.

19.I am generally opposed to Biometric Identification such as for surveillance purposes.

20.Prefer that should be banned, as privacy risks are even more significant (including when controls fail).

21.If selectively use, threshold for use in risk assessment should be higher. Would likely need tighter approaches. Possibly need restrictive controls rather than current self-managed approach in the Code.

I oppose Biometric Categorisation. I partially support the Code
22.I oppose or generally oppose Biometric Categorisation. I partially support the Code.
Results excluded from Biometric Information

23.I note the consultation document summarising biometric information has changed since the last consultation. "The results of biometric processes (match, alert) are no longer part of the definition of biometric information and not covered by the Code".

24.Regarding Q7. "Do you agree with the definition of biometric information and related terms (biometric characteristic, sample, feature and template and result)?"

25.I haven't looked at the previous consultation for further information why result is removed from the definition of Biometric Information. (Due to lack of time.)

26.I also note in this version of the Code result is defined as personal information.

27.In my opinion, result should be classified as biometric information, as it is personal information derived from biometric information. Whilst the results do not carry some of the same risks as does the biometric information, as part of the biometric privacy risk, the results themselves as an output can be a significant privacy risk.

I partially support Rule 1 Purpose of collection of biometric information

28.I generally support Rule 1 as a heightened requirement (for biometric processing), as compared with the Privacy Act Information Privacy Principle 1.

29.I support Rule 1 subrule (1).

30.Regardless of Rule 1 subrule (1), I strongly encourage defining Proportionate in the Code section 3. I note the Code guide seeks to discuss Proportionality.

31.Regardless of Rule 1 subrule (1), I encourage defining Necessary in the Code section 3.

32.Regardless of Rule 1 subrule (1), maybe define Effective in the Code section 3.

I prefer "outweighs the privacy risk to a substantial degree" as part of Rule 1 proportionality
33.Regardless of Rule 1 subrule (3)(b), I encourage defining Outweighs in the Code section 3.

34.I oppose Rule 1 subrules (3)(b), (4), (4)(a) and 4(b). I support the phrasing in Rule 1 subrule (4)(c) "...outweighs the privacy risk to a substantial degree". I believe it important to identically expand outweighs in Rule 1 subrules (3)(b), (4)(a) and 4(b). I believe it important to similarly expand outweighs Rule 1 subrule (4) wording (or alternatively there are other ways in that subrule (4) or introducing substantial).
(3)For purposes of subrule (1)(c), the agency must take into account the following factors—

(a)the scope, extent and degree of privacy risk from the biometric processing; and
(b)whether the benefit of achieving the agency's lawful purpose by means of biometric processing outweighs the privacy risk to a substantial degree; and
(c)the cultural impacts and effects of biometric processing on Māori.
(4)For purposes of subrule (3), the benefit of an agency achieving its lawful purpose outweighs the privacy risk of biometric processing to a substantial degree if, in the circumstances—
(a)the public benefit outweighs the privacy risk to a substantial degree; or
(b)a clear benefit to the individuals concerned outweighs the privacy risk to a substantial degree; or
(c)the private benefit to the agency outweighs the privacy risk to a substantial degree.

I'm short on time for this submission; briefly mentioning some other important concerns
35.Proportionality statement available essential

36.Proportionality statement insufficient. Supporting information.

37.Suggest Privacy Impact Assessment mandatory, and available.

38.My concern is often the justifications and analysis are incorrect / poorly conducted / falsehoods / very biased. Despite some appearance of a Privacy Impact Assessment. Even where organisations have informed the Office of the Privacy Commissioner.

Errors & omissions excepted [ENDs]