Submission to the

The Office of the Privacy Commissioner

on the

Targeted engagement: A potential biometrics code of practice

4th September 2023

About Digital Identity NZ

DINZ is a not-for-profit, membership-funded association under the New Zealand Tech Alliance. DINZ is an inclusive organisation bringing together 80+ members from private, public, and NGO sectors with a shared passion for the opportunities that digital identity can offer. It supports a sustainable, inclusive, and trustworthy digital future for all New Zealanders through its vision — that every New Zealander can easily use their Digital Identity in its mission to empower a unified, trusted and inclusive Digital Identity ecosystem for Aotearoa New Zealand that enhances Kāwanatanga (honourable governance), Rangatiratanga (self-determination and agency), and Ōritetanga (equity and partnerships).

DINZ is the voice of digital identity in Aotearoa. It hosts the annual Digital Trust Hui Taumata, undertakes research and reports on the state of digital identity, makes submissions on digital-identity-related consultations and provides a forum for discussion, new technology, and new initiatives to advance digital identity in Aotearoa to enhance privacy and security for all New Zealanders engaging in the digital economy.

Summary commentary

1. This submission is the result of a collaborative Special Interest Group effort amongst DINZ members, subject-matter experts in privacy and biometric technology (including a number on its Executive Council) and invited experts from indigenous backgrounds. In particular, DINZ thanks Kiya Basabas, indigenous to tribal groups in the Philippines, an indigenous rights advocate and works with Māori data experts in this space, and thanks also Dr Warren Williams, CEO of 20/20 Trust for his expertise and insights into Māori tikanga and Māori Data Sovereignty that hugely informed this submission.

2. DINZ appreciates the time extension granted by OPC in what is a long paper with its requisite list of questions. While DINZ appreciates that there will be further opportunities to provide feedback, we would like to build on important points already raised in our earlier submission.

3. DINZ believes that the Privacy Act 2020, with the provisos that Privacy Impact Assessments become mandatory and that really high-quality guidance is published with close oversight by OPC, is adequate to provide appropriate privacy protections in the field of biometrics. In May 2022, the Singapore Government published this guide: Responsible use of biometric data in security applications which could be used as a starting point reference if the OPC decides upon co-created guidance, although it is appreciated that the scope would have to be wider and the detail deeper if it is to achieve the goal desired by DINZ. DINZ notes that the limits placed on OPC's scope restrict it from engaging a broad spectrum of controls, most of which are technical in nature. The Privacy Act is by and large enabling and protective and sensible (and both world-class and internationally interoperable in useful places). With the Privacy Act 2020 as the fulcrum, *together with mandated PIAs*, good guidance, and close oversight, the whole industry is lifted to a higher bar of knowledge, poor practice detected in a small minority of outlier implementations can be mostly curbed, and where exceptions continue to exist, then a Code could be applied to the exceptions.

4. Definitions: OPC's introductory commentary and discussion of definitions has given DINZ cause for concern whether the topic area and its scope are following a logical and consistent path towards a regulatory environment that allows easier comparison with key international regulatory regimes in the European Union and other jurisdictions. Multiple responses on this matter of definitions throughout the detailed questions Q1–Q57 is indicative of just how much of an issue DINZ believes it is. Until there is consensus on which of the international definitions will apply in New Zealand, there can't be meaningful engagement to move forward and to introduce a code in such an environment takes the topic to an altogether higher level of risk. The high-level analysis shown in the Addendum at the end of this response is a starting point.

5. DINZ's concern with 'categorisation': Introducing a code for 'categorisation' is not consistent with major overseas privacy regulations and introduces confusion around the purpose and use of biometric information. All other jurisdictions have focused just on Identification and Verification uses of biometric information in their guidance and regulations. These are the only areas where the technologies can have a distinctive impact on an individual's privacy. They have all decided not to progress with targeted privacy regulation outside these two areas. OPC is considering provisions that other nations have discounted. DINZ agrees with research done for other nations, which has determined the personal and social concerns should be about agency use of all personal information, not just biometric data. By proposing the IPP changes include "any uses", the proposed code is exceeding OPC's legislative mandate as well as the scope of the discussion document. Consequently, we encourage OPC to consider narrowing the focus of any IPP changes to solely protect the privacy of the individual in relation to Identification and Verification. As currently worded, OPC is proposing regulatory changes that would intrude into the domains of other regulatory authorities, or would create new law outside the reach of the Privacy Act.

6. Māori data: It is important to note that we have a reference to Te Tiriti o Waitangi, as a founding document of Aotearoa New Zealand, and that it acknowledges the partnership

between Tangata Whenua (Māori) and Tangata Tiriti (Non-Māori). For this document, responses from Tangata Whenua are underpinned by cultural values and perspectives, and so those responses aim to provide a space for and the basis of further conversation. In relation to identification for Māori, there are many culturally-based identifiers that link to the physical and spiritual essence of a person. For example, these may include (but not limited to) imagery - facial and body expression, tattoos; and verbal - language, dialect. DINZ has provided responses to the question on Māori data compiled by our indigenous participants one of which is of Māori descent, provided in the Introductory sections and 'Some Questions to get you Started' section as well as in Q 50 and elsewhere on this vitally-important aspect.

7. DINZ's view of a proposed code: DINZ's position remains the same as it was last year and it is still our strong belief that the New Zealand Privacy Act 2020 is an effective framework for regulating biometric information. OPC guidance indicates that "certain types of personal information can generally be regarded as sensitive if the inferences that can be drawn about the individual from that information are potentially sensitive[1]", and we expect that a good deal of biometric information can be regarded as sensitive. We urge the OPC to take a measured approach and not rush into providing a code. That 'there was roughly equal support for further guidance and for a code of practice under the Privacy Act' speaks volumes to the concerns raised by interested parties and that a rush to a code will result in a change to 'compliance behaviour' that will stifle innovation, have unintended consequences, and negatively affect the positive outcomes sought by a code's introduction.

8. Guidance is the best way forward in the near term: DINZ reiterates its suggestion from last year, that the OPC develop guidance on the use of biometric information in Identification and Verification, co-created with industry experts so as to not only help ensure that the guidance is informed and useful, but also improve OPC's own internal operational expertise bench-strength. This should also reference international standards on biometric information and technology (see listed in Question 3). As it submitted last year, DINZ believes that a lot more can be done to guide, support, and nudge organisations and their staff implementing biometrics towards best practice, in particular where the field of biometrics is new to them. While DINZ acknowledges OPC is trying, and agrees with many of the remarks made by OPC in the paper, it remains concerned that the remarks don't exhibit sufficient knowledge of the potential unintended consequences of taking a particular path – 'a little knowledge is…' and so on. Where guidance is published by OPC, take Multi-Factor Authentication as an example, the quality and actionability of that guidance implies that it was not co-created with industry (certainly not with the country's only dedicated industry association for digital identity at least), which exacerbates the concern about OPC's capacity and capability in matters that are extremely technically complex in nature.

9. Biometrics improve the digital experiences of New Zealanders every day in both the public and private sectors. Demonstrable privacy and technical expertise – alongside practical

---

1 https://privacy.org.nz/assets/New-order/Your-responsibilities/Privacy-resources-for-organisations/Sensitive-Personal-Information-and-the-Privacy-Act-2020.pdf

experience the likes of which are found in DINZ members – combined with good design and implementation are keys to great outcomes. So please leverage them to iteratively lift the skill and knowledge baseline in Aotearoa.

Colin Wallis
Executive Director
Digital Identity New Zealand
New Zealand Tech Alliance, PO Box 302469,
North Harbour, Auckland 0751
E | colin.wallis@digitalidentity.nz
M | +64 21 961955

4 September 2023

DINZ comments on the introductory sections:

What's this about?

In this section, the second paragraph states 'What is OPC looking for from stakeholders?'

Māori data

[....]

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

DINZ high level comment informed by Māori Participant :

Generally, many of the concerns expressed by Maori are relevant to other groups in society. Māori are a strong vanguard on these issues. An important question is whether addressing these concerns would benefit all of society or should be a unique consideration under Te Tiriti o Waitangi. The general concerns expressed by Māori are not unique in the world and have been explored in depth overseas for other cultures. In general, biometrics enable recognition and respect as an alternative to traditional identification and classification. In very simple terms - "you are you" because I hear the intonation in your voice, I see the shape of your facial features, the spiritual state of your ancestors in addition to your physical state rather than "you are the person identified and classified by someone else". The former is a better environment. There's a positive impact assessment that needs to go alongside the risk impact assessment.

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

- the scope of a code, which is proposed to cover the use of biometrics to categorise people as well as to identify them

DINZ high-level comment

The term used overseas is "distinguishing identification" to determine if someone is part of a particular group. This has the potential to have the greatest positive impact on privacy, as it enables agencies to work with people without necessarily identifying them. Avoiding unnecessary identification is the most impactful thing a business can do to improve privacy for its staff or customers. While distinguishing identification can be used by bad actors to cause harm to individuals, that concern is not limited to biometric information. Current PIA practices require agencies to do the right thing — this proposed code doesn't appear to change anything. This is why we have suggested mandating PIAs is the starting point, with a suggestion relevant to this question, that a PIA include an indigenous impact and consider explicitly the detection and mitigation of any potential bias, harm, or unintended consequences. That could start off as guidance and later be included in changes to the Privacy Act perhaps?

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

Question

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

DINZ Comment from Indigenous participant:

[While accepting that this following comment might be considered out of scope for this consultation].. Create a separate Māori data privacy code or Māori information code at a higher level (maybe at a foundational layer in the Privacy Act itself?) that has legal effect, which safeguards the use of Māori data from a tikanga lens in many applications (specifically the issue of secondary use). Guidance or if it came to it, a biometrics code could then apply this as would other codes (e.g. Health).

DINZ Comment from Māori participant:

Kia ora, I am of Maori heritage and work in the Māori Data Sovereignty space as well. It's important that an indigenous/Māori worldview/perspective is incorporated as it is indigenous/Māori peoples that are subjected negatively due to breaches of privacy, inappropriate profiling and similar activities where technology is misused or abused. While I am not against biometric technology, past system process/policy failures have resulted in too little or low consequences on those creating the breach of controls, etc. This is where many indigenous people are wary of new technologies as they have not been favourable to them in the past. (e.g theft of IP/image/voice/taonga/etc etc). Control, access and protection are key but the lines of jurisdiction (or lack of) also creates concerns. How to solve I'm not sure.

Overview of proposals

What would a potential code cover?

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

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

A code would apply to all of the organisations that have to comply with the Privacy Act, if they are using biometric information in automated processes.

DINZ comment:

These examples are all of quite an active nature, whereas some of the examples given in the previous paragraph are of quite a passive-biometrics nature. This dimension is important (as is the context in which biometric information is acquired or observed), and it feels like there will be conflict and contradiction with aspects of the code such as consent and purpose (below). Where does this leave passive-biometric observation in anti-fraud situations such as attributing risk factors to authentication on the basis of keystroke rhythms for example?

Active versus passive collection of biometrics is something that can be clearly specified and understood. DINZ's research for this consultation evidenced that consent for active collection was easy to work into processes, so informed consent is possible. Notices about passive collection were acceptable as long as people had an alternative option. In both cases, the data subject needs to have a way to opt out of course, otherwise the company collecting the biometrics gets in trouble. In practice this is not working well overseas with some unintended consequences. The cases looked at resulted in non-compliance infringements but no harm to actual privacy described. The worst case stopped universities in a country from offering online proctored exams during COVID19 lockdowns because there wasn't an alternative.

What would a potential code do?

[...]

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

DINZ comment:

The use "proportionate" is interesting here, given the likely subjectivity of what is proportionate and given the likely shifts over time that should reasonably be expected in both what service providers, agencies, and citizens think is proportionate (i.e., in order to gain secure access to important things, and in order to have meaningfully-better experiences and conveniences).

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

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

DINZ Comment:

What is "marketing" from a testable-definition perspective? For example, would benevolent targeted population-health messaging from Te Whatu Ora be considered "marketing"? (definitions). Further, if individuals are willfully opting in and giving meaningful consent (with or without financial or other fair and reasonable incentives for doing so) is it sensible that this kind of thing is prohibited?

As regards emotions or health information, if deemed ethical, there could be significant and positive outcomes for health, safety, and wellbeing by doing exactly this kind of thing in a wide range of settings, potentially controlled or hazardous settings (e.g., building sites, factories, airports).

As raised above, these are potentially good reasons to have a code of practice, but also not things that are limited to biometrically-enabled use-cases, so therefore *not a biometrics code of practice*. Approaching it in that way puts any potential benefits and protections beyond reach, when they could be doing a huge amount of good.

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

[....]

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

DINZ Comment from Indigenous participant:

Individuals should also have the right to refuse giving their consent without prohibiting their access/entry/etc. e.g., people currently being refused entry into bars if they do not get their face photographed, even if they are not on a watchlist etc.

More specifically:

- They would need to be told about how the organisation will handle their biometric information before being asked to give consent. The organisation's handling of biometric information would need to be explained in ways that mean that the person understands the potential consequences of the use of their biometric information.
- They would have to clearly agree to the collection – an organisation couldn't just assume collection is OK unless the person objects.
- They would have to agree separately to each purpose, if an organisation will be using their biometric information for more than one purpose.

DINZ Comment:

That individuals agree separately to each (new) purpose for which their biometric information is used and consumed is naturally good, and sensible from a Privacy Act perspective. However, this expectation can perversely incentivise bad behaviour around the scope-setting and nature of consent acquisition by creating an environment in which individual consent is defined murkily and with all-encompassing opportunistic scope, claimed to avoid the need for reconsenting in the future. If this is a code for Aotearoa then can there be something bold done (privacy dashboard software app for example) and a series of acceptable-and-expected use-cases defined well-enough that consent can be given sensibly and once, and reviewed at any time by the person giving consent?

- They would need to be given an alternative to having their biometric information collected (unless it's really not practical to do so), so they have a genuine choice.
- They would have to be allowed to withdraw their consent later on, which would mean the organisation would have to stop using their biometric information and would need to delete it in most cases.

DINZ Comment:

Not at all specific to biometrics, but "delete" and adjacent electronic recordkeeping terms such as "destroy" can be a challenging concept in a digital landscape filled with robust backup-and-archive systems and processes and the prevalence of everything-as-a-service consumption models. We suggest this terminology be reviewed and amended to something more actionable such as "archived" or "rendered unavailable for processing".

DINZ Comment from Indigenous participant:

Further to this, OPC should consider how they delete biometric information, particularly with deceased peoples. In some cases could information (physical or digital) be returned to whānau?

(Note that further down, is the suggestion of separating out deceased people's information from those still living and doing so as part of a ceremony).

[....]

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

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

DINZ Comment from Indigenous participant:

See comment above from Māori participant and given the disproportionate surveillance that Māori incur within state systems, and the amplified risk of experiencing some form of data harm, there is a collective privacy risk of population profiling. It is important that agencies understand their obligations with respect to protecting Māori data privacy; this could be enforced in a PIA if not in a separate code prior to potentially changes in the Privacy Act?

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

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

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

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

DINZ Comment:

We've found the use of the term 'share' difficult to parse but we think it means transfer to another entity for further processing. Note the potential relationship to the MBIE *Consumer and Product Data Bill*. In that bill the data holder must share customer information with accredited requestors if agreed by the individual.

There's also a big difference between "someone" and an "individual". Someone may not be identified: e.g., the student in Seat C4 is someone, but Bob the student is an individual. "Someone" is not a great word to use in this context, however we assume the intent is that this term is to refer to an identifiable individual.

Make sure there are proper security safeguards for biometric information

[....]

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

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

DINZ Comment:

Significant issues arise here about the actionable definition of "stored separately" and *exactly* what comprises "biometric information" and *exactly* what comprises "other personal information". These questions are all solvable, while recognising that for biometrics to play a useful and benevolent role in many scenarios there must be a resolvable identifying link established between the (separate) biometric store and all the other information stores.

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

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

DINZ Comment:

The expectation of "deleting" raw biometric information is couched in terms of whether or not there is a good reason to keep it. What does this mean for an organisation like, say, a University that has photographs of its staff and its students and some other affiliated people, photographs that it prints onto plastic identity cards and photographs that it publishes on its websites that feature the

academic works of its researchers? Is a *photograph* of a person not the same thing as a raw biometric image? If an institution started to use photos like those that it already held for "biometric" purposes then that would be covered by the earlier statements. In the context of human-resources and student-management and identity-card solutions it is not possible to separate "biometric" data such as photographs from other information about individuals, such as their identity details or their employment or their enrolment.

Make sure organisations check the accuracy of their biometric systems

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

DINZ Comment:

What does "accuracy" look like, both system-wide (how good is good-enough?), from one population group to another (how consistent is 'good-enough'?), and are there some population groups for whom accuracy must be very high (e.g., to ensure there is no systemic negative bias)?

The importance of accuracy (and to some extent the importance of equitable accuracy) likely varies by situation: it's one thing for biometric assessment to declare a person is old enough to be admitted unchallenged to an R16 movie, another to waive the need for documentary evidence when purchasing alcohol, another to give somebody access to a bank account, and quite another to grant access to a maximum-level-biological-safety research laboratory.

Errors in identifying people occur regardless of the technology or systems used and have always happened. The concept of 'privacy enhancing' could be useful here - instead of limiting harm from unknown inaccuracy and mistakes, require new technology to be 'Privacy Enhancing Technology' - better than what's in place already.

Some questions to get you started

What parts of our proposals do you agree with?

DINZ Comment:

We appreciate that the OPC has explained in careful detail the various concerns of privacy practices in the use of biometric technologies. The intent and ideas within the discussion document look good, in general, with some suggestions from us detailed in this paper. It is still our strong belief that the New Zealand Privacy Act 2020 is an effective framework for regulating biometric information which is

sensitive personal information. This is a serious topic and we do think proper consideration for the concerns expressed to the OPC is warranted.

We wish to work with the OPC to develop in the interim step practical guidance for agencies to use when adopting biometric technology, mapping out the Privacy Act's Information Privacy Principles (IPP) with considerations and suggestions for agencies to follow. This would bring both increased education around the types of biometric use cases, how the IPPs map to these and what additional considerations agencies should be following which will overall lift the maturity and privacy best practices in the industry. As part of this guidance, the OPC could consider developing a risk assessment framework which outlines in particular where automated biometric technologies and their particular use cases should follow certain guidelines. If such guidance does not yield a positive result in the sector as defined by some meaningful, agreed-upon KPIs, and the OPC continues to get a strong and material amount of feedback from the public, the OPC could then evolve this guidance into a code.

We consider it important that the focus be clearly on biometric information, not biometric technology. The technology landscape is changing by the month such that a code would never keep up, and introduce unintended consequences.

Other jurisdictions do regulate biometric information as personal information (including the template) but in such cases there is much more detail e.g. separating the template from the biometric evidence (i.e., deletion of data policies).

We agree with the OPC that Māori's concerns on use of biometrics should be taken very seriously and in particular with reference to cultural considerations like holding biometric information about ancestors. DINZ proactively seeks the views of our Māori members and stakeholders in these consultations as well in order to establish practical steps to address these concerns with technology, balancing the opportunities of their use with cultural risks and challenges. We think the OPC, if it develops guidance, should adopt a risk-based and principles approach to privacy best practice on biometric information – in doing so, different perspectives including Māori cultural considerations can be incorporated over time as feedback on particular biometric use cases develop in New Zealand. As already suggested, the Privacy Impact Assessment (model template) could also include a cultural consideration aspect to it asking specific questions about handling of ancestor's biometric data.

Are there any red flags in these proposals for you? What are those?

DINZ Comment:

The reference to feedback from Māori and people living with disabilities that the OPC has taken on board will deny valuable opportunities for these groups and others to benefit from the ethical and robust use of biometric identification. We welcome the indication that well-founded exceptions will be considered.

Security over sensitive biometric information is an important consideration but this is important irrespective of where that data is stored. Therefore in reference to Question 43, IPP 12 we have outlined in that question, this must be applied to all personal information equally.

Given the wide definition of biometric information in this discussion paper, it will include the capture of images using security cameras. Taking a broad definition like this will make implementing a code difficult. Instead we recommend this consultation focus on active capture situations (where biometric information is being collected for the purposes of establishing a relationship to the person's identity and automating identification, for example). For example, consent is often not practical for passive capture situations (i.e. CCTV footage). Other legislation provides guardrails around CCTV usage regarding the consent and transparency measures that should be taken, for example, employers in New Zealand can install CCTV in the workplace as long as they inform their employees ahead of time and the employer must comply with the Employment Relations Act 2000 and the Privacy Act 2020.

If this broad definition is to capture a wide range of biometric technologies in a wide range of use cases, we would recommend sector-specific guidance be developed in order to properly capture how the sector is working and dive deep on the privacy practices that should be in place to protect personal information. However this will raise practical issues if there will be a requirement to obtain consent to the collection of biometric information. Careful consideration will need to be given to the proposed exceptions to the consent requirement, and guidance as to when they are intended to apply. For example it should be clear whether "maintenance of the law" would cover a security camera installed for the purpose of deterring stock shrinkage.

The consent requirement is fairly strict. For face recognition the primary use cases are security and crime prevention, and in those cases the criminals and offenders don't usually like to give consent! Whilst the proposed code does have exceptions it would be better to have those exceptions stated more clearly to cover scenarios where face recognition is being used for crime prevention and offenders are being enrolled in the system to help prevent repeat offences. e.g- use in retail to detect previously violent offenders returning to the store.

What concerns you most about what we're proposing?

DINZ Comment:

We think it is too early to introduce a code, that biometric technologies have different risk profiles and use cases and often the context of who is using the biometric technology and for what purpose either increases or decreases that risk to personal information and human rights. We absolutely believe human rights should be fundamentally protected and to do this in an implementable way, which raises the understanding and maturity of the use of these technologies, then a risk-based approach which is sector specific that yields practical guidance will support adoption of good use cases of biometric technologies and heavily discourage improper uses. It is a hard ask and there needs to be ongoing opportunity for feedback and review of the code if it gets implemented and real

use of it is experienced and learned from.

Denying the application of biometric technologies for use in marketing (and we have already expressed concerns about the definitional challenges around what exactly marketing activities relative to the 'marketing-adjacent activities of relationship and engagement communications, particularly where there are material public-good benefits etc where people might wish to opt in to these biometrically enabled services) certain sectors would significantly overlap protections provided in other legislation. We think it would be more appropriate for those regulations to be updated as they specifically relate to the sector. For example:

•Using biometric information to target direct communications with someone would be equivalent to using an email or phone number in direct marketing. The Unsolicited Electronic Messages Act should cover this but may need updating.

•Using biometric technologies in direct selling may be relevant to the uninvited direct selling provisions of the Fair Trading Act. These provisions may need updating, as the place and type of uninvited direct selling may be out of date with newer technologies.

•Intentional harmful use of biometric information would likely fall under the Harmful Digital Communications Act. This act provides a robust enforcement framework that extends from civil action to court orders and into criminal conviction. There is a well established public facing service from NetSafe. Only 10% of cases relate to sensitive personal information - intentional harmful uses of biometric technologies may extend beyond the privacy rights of the individual.

•The use of biometric information in identification and verification (automated) processes is quite targeted, and is the basis of most biometric data protection regulation around the world. This proposal explores a lot of subjects that are outside that scope. The classifying uses of biometrics have been explored and excluded from overseas personal data protection regulation for good reason. Once biometric data is used outside of identification and verification it just becomes personal data, if it's associated with an individual. Any personal data used for classifying people raises the same concerns as biometric data, so there are few specific biometric regulations beyond identification and verification.

•Biometric technologies and information have a lot of uses that are not associated with an identified individual. This proposal does not consider this carefully, and uses language that assumes every use is personal to an individual. There are plenty of scenarios where biometric technologies can reduce the need to identify individuals, which can profoundly improve privacy and trust.

•The unintended consequences of the proposal are pretty significant. Take this as an example: OPC would have to manage a large exception where many consumers could benefit from getting better outcomes such as being recognised as someone who is unhappy with the service received when talking with a Bot or an Agent or being offered age appropriate options. Humans make assumptions based on a combination of the words spoken and the vocal characteristics to guide a customer to the most appropriate offer. Bots (and humans) will be more effective if biometric indicators of emotion or age can be used to improve service. This form of biometric does not even need to be "identifying " an individual.

Did we miss anything out? What do you think that is?

DINZ Comment:

We encourage the OPC to highlight in these consultations and any possible guidance that biometric technologies play a key role as a means for multi-factor authentication (MFA) and that, as per the OPC's guidance on MFA in June[1], MFA protects against privacy breaches. We have seen, for example, the Australian Government make such recommendations in relation to use of biometrics in verification of identity with consent to improve resilience and make it harder for criminals to misuse identity credentials.[2]

[1] Office of the Privacy Commissioner encourages two-factor authentication in war on cybercrime, June 2023 https://www.privacy.org.nz/publications/statements-media-releases/office-of-the-privacy-commissioner-encourages-two-factor-authentication-in-war-on-cybercrime/

[2] National Strategy for Identity Resilience, Australian Government, June 2023 https://www.homeaffairs.gov.au/criminal-justice/files/national-strategy-for-identity-resilience.pdf.

The Privacy Act focuses on the privacy impacts of the handling of information, therefore if the impact arises in a manual or automated-manual "hybrid" context, it should be caught by the Act / code / guidance. There seems to be an underlying assumption in the paper that everything transacted manually by a human is highly-accurate and unbiased, which is simply and grossly untrue. Ignoring these scenarios will create an undermining blind spot in the guidance and render it of limited usefulness. Consideration should be given to the manual processes associated with either making identity decisions or assessing the outputs of automated biometric matching. Insufficient rigor and quality assurance in this realm can similarly introduce systemic bias / noise in the identity management process. The false perceptions that biometrics are uniquely risky or that they present risks that aren't present with alternative service delivery models (like purely biographical identity management, or human-only processes) should be also dispelled.

Have you seen biometrics done well anywhere that you'd recommend we look at?

DINZ Comment:

OPC is already aware of the following but:

- Inland Revenue has been using Voice Biometrics for over 15 years?
- Police have been using fingerprinting for many years as well?
- NZ Customs Smart Gate?
- Apple and Samsung Face and Voice Recognition?

Is there anything that we've really missed the mark on? What is it?

DINZ Comment:

- By addressing concerns of some parties, the benefit to others may be impacted and also may miss positive discrimination opportunities.

- We recommend that the OPC's definition of "biometric information" be aligned with the International Organization for Standardization (ISO), as this reflects an international and long-standing approach to creating standards and regulating biometrics. ISO defines biometric characteristics as "biological and behavioural characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition". This aligns with the NZ Privacy Act - information is personal information when it is information about an identifiable individual. Likewise, sampling of traces to obtain biometric information could be a strand of hair on the bus, a fingerprint on a public toilet's door knob, but this is arguably not private or 'personal' identifiable biometric information. Instead from a practical perspective, it is where there are "distinguishing, repeatable biometric features that can be extracted for the purpose of biometric recognition".

- Are biometrics on a smartphone in scope? Just imagine asking customers for consent for each different use case of the biometrics to unlock the phone, to pay a bill, to unlock your holder app, and so on. This is actually the biggest area of concern at the global level although potentially improved from July 2023 with the EU-US cross-border data protection being agreed. Has OPC materially explored this so far? After all, smartphones have the front-end hardware and software most likely to be used in biometric sampling for identification and for verification. If the smartphone vendor does anything with the data collected (digital images/filters of moko being misappropriated on social media sites for example), then they would have to be considered to be within scope of any proposed code.

What is the most important part of this work for you?

DINZ Comment:

• Providing clarity about what is and what is not compliant, and assistance / guidance on how to implement Biometric solutions accordingly.

• If there is a decision to proceed with a code (despite the obvious reluctance of industry to do so at this time) the extent that aspects fall under a Code vs Guidance (DINZ) must be clear and helpful to an Agency looking to implement Biometrics. (example of AML/CFT Code of practice still left a lot of room for interpretation and in some cases confusion. Good testing of the Guidance (or Code if it came to that) before publishing would be beneficial along with the opportunity for regular updates based on feedback.

The proposals in detail

Scope of a code

Biometric information is information about people's physical or behavioural characteristics (such as a person's face, fingerprints, voice or how they walk).

DINZ Comment:

The GDPR definition* of biometric data is by far the most developed and practical to apply, even if not the ISO definition, but both should inform OPC's approach much more than is apparent.

Two main issues:

1. Personal data is not necessarily private. The Privacy Act conflates the two, making its application to biometric data a bit more difficult. The analysis in the Addendum tries to wrap the biometric data with classification types, rather than fixing the ambiguity in the act.

2. Personal data protection is slightly different to 'privacy', so the goals of the OPC are not quite the same as the EU. That is understood and accepted. But as a result, the OPC proposal extends its reach into derivative information from the original biometric data. Consequently the edges of OPC's definition are much broader than GDPR - for example standard data management and analysis tools and information artifacts are in scope for OPC.

*For easier reference: 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" from #14 in https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1489-1-1 noting also that DINZ has included a reference to the EU/GDPR Biometrics Working Group document from 2003 in the Addendum+definitions at the end of this response.

Questions

Q1: Do you agree with the proposed scope of a code, including proposals that it should apply to:

- *all agencies covered by the Privacy Act, to the extent that they are using or intending to use biometric information for automated verification, identification or categorisation of an individual*
- *information about physiological and behavioural characteristics*
- *biometric information that is to be used for automated processes*
- *biometric information that is to be used for the purposes of verification, identification and categorisation*

- *biometric samples (raw biometric data, where that data is to be used for automated biometric processing) and digital biometric templates?*

DINZ Comment

No

We recommend that before the OPC makes a decision on who is covered by the code, the OPC develops what necessary guidance and best practices agencies should be using with respect to biometric information used in automated verification or identification of people. Introducing privacy requirements around biometric information used for categorisation is out of step with all other major biometric regulations overseas. In testing this guidance and best practices, drawing from international standards, the OPC could determine common use-cases where those biometric technologies are being used in automated processes on personal information that pose a privacy risk to New Zealanders' personal information. Working from these use-cases is vastly preferable to developing a top-down privacy code that applies to all agencies uniformly yet is impossible to be made evenly applicable. Identification of use-cases followed by development of a risk-assessment framework either in addition to or conjunction of the Privacy Impact Assessments would support a risk-based approach to regulation of biometric information.

As OPC outlined in the 2022 position paper, the regulation of biometric information operates through a number of relevant laws including the New Zealand Bill of Rights Act, Immigration Act 2009, and other standards, including the Cross-Government Biometrics Group's *Guiding Principles for the Use of Biometric Technologies for Government Agencies* in 2009. It would be useful to develop practical guidance to support entities in navigating the various regulatory requirements.

We recommend the OPC align its definition of "biometric information" for the purposes of this consultation to the International Organization for Standardization (ISO). ISO defines biometric characteristics as "biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition"[2]. In particular, the OPC has identified a range of biometric use cases which are broad and potentially not limited to determining the identity of the individual unless that individual's personal details are collected and bound to that biometric raw data – we would suggest that such a broad definition of biometric information makes the practical application of such guardrails difficult.

We agree that biometric information that is being automatically processed needs particular guardrails for the proper development of that technology to avoid harmful bias. In particular, we would recommend that confidence scores be utilised. The use of confidence scores is an example of a good practice to inform how much trust can be placed in the results of any technology. Where the risk is higher, higher confidence scores could be set, for example, as best practice in any guidance OPC could jointly develop with various stakeholders and industry.

[2] https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en

That said, hybrid systems need to be in scope as well at the barest minimum. Not considering purely manual processes seems contrary to the intention of the Privacy Act itself that is concerned with the impact of the use of certain types of information.

Where biometric information is used for the purposes of verification, identification and categorisation the intentions of the New Zealand government to develop the Digital Identity Services Trust Framework (DISTF) is relevant to this work and any guidance should be in alignment with the DISTF Act and subsequent regulations to ensure any mismanagement of biometric information is being addressed through those rules.

If the OPC chooses to focus on how agencies use biometric information in its original state (raw biometric data etc.) and the privacy controls around collecting, storing, sharing, processing of that information, we note that privacy impact assessments (PIAs) should be adequate as being in scope and do agree with the OPC's recommendation to publish a model PIA for agencies to use. PIAs should take into consideration the scale and likelihood of possible privacy impacts and where possible, without prejudicing the commercial sensitivity of a project, be published. For example, with the COVID Vaccine Pass, Manatū Hauora (Ministry of Health) proactively published a PIA to demonstrate how technology providers were providing this solution and how the personal information of New Zealanders was being processed and stored.[1] This proactive publication was well received by various stakeholders and we would suggest this serves as a good example of how PIAs can be proactively published to explain how technology providers are respecting the New Zealand Privacy Act 2020.

---

[1] Ministry of Health, National Integration Applications – formerly known as the COVID-19 Technology Integration Product (CTIP), August 2022, Ministry of Health https://www.tewhatuora.govt.nz/assets/For-the-health-sector/COVID-19-Information-for-health-professionals/privacy/NIA-API-Privacy-Impact-Assessment-PDF-749-KB.pdf

Q2: If you think a code should apply to a narrower range of agencies, which types of agencies or sectors should it apply to, and why?

DINZ Comment:

DINZ recommends avoiding a private/public sector-specific split, but rather industry sector-specific because there is a risk that the private sector would potentially exploit it if the guidance existed only for the government agencies, and conceivably it would be easy to misinterpret any remaining low public trust as a sign of government needing even stronger legislation — as opposed to guidance issued for an industry sector.

In DINZ's opinion, OPC's concerns are lightly evidenced (references to concern, fear, and possibility but not meaningful impact assessments, KPIs, or any tangible evidence, even if that were just the number of compliance actions received / investigated by the Privacy Commissioner per year), so currently we likely cannot predict exactly what would shift public perceptions. But the prospect of a

government agency having a different set of rules to a private company in the same industry sector would surely not help shift public perceptions.

Q3: How should a code deal with biometric information that is held for both manual and automated processes, or for hybrid manual/automated processes?

DINZ Comment:

We suggest that useful guidance, co-created with industry (DINZ, Standards NZ, CGBG, NZ members of ISO/IEC JTC 1/SC 37, etc) should reference similar guidance and standards that have been set at the international level. These standards which have been developed including New Zealand biometric experts can serve as a useful reference point. This would include, for example, guidance around setting confidence scores in the use of automated biometric technologies. Some examples of standards include (but there are many, many more):

• *ISO 19795-1:2021 Performance Assessment:* This standard establishes general principles for testing the performance of biometrics systems in terms of error rates and throughput rates.

•*ISO 19795-10 Differential Impact/Bias:* This standard is still in development and is not yet published but includes biometric performance testing and reporting – quantifying biometric system performance variation across demographic groups.

•*ISO 30107:2023 Presentation Attack Detection:* This standard establishes principles and methods for the performance assessment of presentation attack detection (PAD) mechanisms, along with a classification of known attack types.

•*ISO19989:2020 Security Evaluation of Biometrics:* This standard extends the security functional requirements of the more general evaluation criteria for IT security (15408) associated with performance and presentation attack detection errors in biometric systems.

•*ISO24745:2022 Biometric Template Protection:* This standard provides requirements for secure and privacy-compliant management and processing of biometric information, covering threat analysis, identity binding, and application models, and guidance for the protection of individual privacy.

•*ISO24741:2018 Biometrics Overview and application:* This standard provides an overview of biometrics and a reference architecture to establish a shared understanding of biometric technology. It also provides information about the application of biometrics in various business domains such as border management, law enforcement and driver licensing, the societal and jurisdiction considerations that are typically taken into account in biometric systems, and the international standards that underpin their use.

•*ISO24714:2023 General Guidance for Biometrics:* This standard provides general guidance for the stages in the life cycle of a system's biometric and associated elements. This document is intended for

planners, implementers and system operators of biometric applications.

•*ISO 2382-37:2022 Information technology — Vocabulary — Part 37: Biometrics*

Q4: If you think a code should apply to a different set of information, which information should it apply to (or not apply to), and why?

DINZ Comment:

As previously stated, biometric information alone (i.e. a fingerprint or a voice template) is not information about an identifiable individual, and as such does not fall within the definition of personal information under the Privacy Act. Biometric information could, and often should, be treated differently than raw identifiable samples like a facial photo.

Algorithmic solutions that compare two templates and return a similarity score are basically sophisticated statistical aggregates of all training and tuning information that was used in the creation of said algorithm. Assuming the guidance intends to remain technology-neutral, this statistically-digested aggregate of biometric information would be well outside the scope.

Q5: Do you agree that a code should not apply to information covered by the Health Information Privacy Code, DNA profiles and genetic information, information from human tissue, and neurodata?

DINZ Comment:

If a code prohibiting health information from being collected or determined were to be in place, certain exemptions would be critical so as to not undermine various medical functions, and the Health Information Code should be meaningfully deconflicted with a proposed code and robust guidance.

Carve-outs introduce complexity in implementation and regulation. It is not clear why information covered by other codes is not excluded from scope, for example the Credit Reporting Privacy Code or the Emergency Management Code.

We acknowledge that neurodata and neurotechnology ("specifically [...] gathering, analysing, and using information that is directly produced by the brain and nervous system"[3]) are immensely-complex emerging-or-futuristic areas of scientific activity about which a wide range of opinions, aspiration, and controversy exist. Both concepts suffer from definitional, scope, and applicability problems that render futile any contemporary discussions about "neuroprivacy". Nevertheless, if “neurodata” are excluded from the OPC thinking about biometric information then many quite-legitimate and high-value uses could be ruled out unintentionally.

[3] https://ico.org.uk/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology/

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

DINZ Comment:

We understand that the storage of data about deceased persons can be particularly sensitive for Māori and recommend where possible that Māori be involved directly in the development of projects where Māori ancestral data are being collected and stored. Clear demonstration of the need for and use of these sacred or tapu data should play an important consideration in the development of such biometric technologies and be reflected on in a Privacy Impact Assessment which could allow for a cultural impact assessment as well.

We have suggested elsewhere the notion of a ceremony to deliver deceased persons to a separate database from the living, though there may be significant practical challenges. We are aware of OPC's publication https://www.privacy.org.nz/blog/privacy-beyond-the-grave/ and comments elsewhere about the potential need to store biometrics (and other?) information about deceased people in a different database and therefore the need to recognise the "mixed" nature of personal data that are biometric data. Biometric information cannot be thought of as "merely" information about an individual person.

DINZ Comment further informed by Māori Participant:

There is a custodial approach to postmortem privacy that should be respected from a legal perspective. Either the wishes of the deceased or their closest relatives should be directing how someone's digital legacy is handled. This is an area of weakness around the world. Biometric data is only a tiny part of someone's digital legacy. Postmortem privacy is worthy of its own code of practice/guidelines. We don't think it does the topic justice to just look at it through a purely biometrics perspective. Furthermore, it's not clear how the inclusion would fit with the definitions of 'personal information' and 'individual' within the Privacy Act itself.

Q7: Do you agree that, before collecting biometric information covered by a code, agencies should be required to assess the effectiveness and proportionality of this collection in relation to the proposed end use of that information?

DINZ Comment:

No.

As stated, we do not agree, because it is not clear what these additional requirements would add. Proportionality is implicit in only collecting information that is necessary. It is not clear what 'effectiveness' means in this context, but the accuracy principle should sufficiently prevent use of ineffectively-collected information.

We have already suggested that PIAs being required, could be more than sufficient to alleviate the conceptual concerns here.

It is important to avoid the development of one-size-fits-all assumptions across different biometric technologies and many different use cases. We recommend the OPC consider developing practical guidance for PIAs that can help entities determine readily the risk profile of different biometric information use cases and determine if collection of biometric information or an alternative method for verifying identity is possible in achieving the same end result. In most cases, biometric information is being collected for a specific and determined use case and is a powerful tool in helping to, for example, establish proof of identity in a multi-factor authentication (MFA).

Q8: How might an agency demonstrate that it has assessed the effectiveness and proportionality of its proposed collection and use of biometric information covered by a code?

DINZ Comment:

As already stated, if the OPC developed guidance and templates for the creation of fair, useful, and robust Privacy Impact Assessments (PIAs), agencies could demonstrate good-faith engagement with privacy concerns without significant effort. It would be unreasonable and, in many cases, extremely cost-prohibitive to require any quantitative assessment of any potential implementation of an automated biometric system at only a conceptual stage.

Q9: Do you think there should be any exceptions to this requirement for particular uses?

DINZ Comment:

If easy-to-follow materials were created that made PIAs accessible to all agencies without the requirement for internal expertise on the process, it would be reasonable to suggest that any agency considering biometric collection and use could undertake one.

It might be reasonable to issue guidance that agencies should not implement technological solutions that they cannot reasonably maintain over time, proportionately to their use-case, but not all use-cases would require the same standards, and therefore may require exemption depending on the rule. Industry sector-specific or use case-specific rules may alleviate this concern.

For example, where an agency uses a third-party service it is likely that the agency will not have control over the composition of information collected. A standardised service may gather more information than the agency needs at that time. The agency can make the assessment and manage risks accordingly, but any compliance requirement to only collect what is needed may create unjustified difficulties.

Q10: Should a code provide for proportionality assessments to be undertaken at a sector rather than an agency level in some cases? How might this work?

DINZ Comment:

This level of detail should not be in a code. In practice, an agency or company should be free to adopt whichever assessments are appropriate for their purposes. The law does not need to provide for that, but it could be a topic in Guidance.

The notion of proportionality is well-described and well-understood at an abstract and legal-technical level[4]. However, we see clearly that individuals will consent proactively and opt willingly into a very-broad range of use-cases where their biometric information will play a central role in creating utility, convenience, and value that enable new human experiences and new service affordances. The resulting opportunities are real and meaningful, and any determination of proportionality can be made only by the individuals participating in a well-informed and strongly-assured Privacy ecosystem.

Q11: Should any purposes for the collection of biometric information covered by a code be ruled out altogether, or is the proposed requirement for a proportionality assessment enough?

DINZ Comment:

Any purpose ruled out would be predictably based on current-state use and current-state technological advancement, which cripple technological innovation and progress in the very same contexts unnecessarily.

Additionally, it is not clear why individuals should be prevented from freely consenting to use of their biometric information for any purpose. Particularly where the basis of that consent is, and should already be, actively regulated.

There are important distinctions between intended use, misuse, and abuse of technologies. Outright banning of intended uses is appropriate if there is a high likelihood of consequential harm from that intended use. If misuse can result in harm, then policies and practices to mitigate risks and minimise incidents are appropriate. If abuse is likely, then risk avoidance or elimination strategies are required.

[4] https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

Q12: Do you agree that agencies should not be allowed to collect biometric information covered by a code for:

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

DINZ Comment:

No, we do not agree.

Sector-specific codes or guidance may be a useful way to develop a more in-depth review of the particular use cases and safeguards for applying biometric technology rather than carving out areas where biometric information should not be allowed to be collected. Where, for example, discriminating on age may however be a legal use-case for biometric technologies — for example, in the selling of vaping technologies to children under the ages of 18 — biometric information may be useful in the classification and determination of age for the case where children are or are not permitted access into certain premises. Taking a one-size-fits all approach prohibits innovation and access to technologies that serve the public interest, not inhibit it. Furthermore, in the case of marketing there are a number of mobile applications that, with the customer's consent, will capture biometric details such as face shape, body shape, and skin tone in order to provide recommendations on fashion, wellbeing, eyeglasses, etc.

It is not clear what the actual "case" is for removing an individual's agency in relation to use of their information. The document simply states there is a case based on the sensitivity of biometric information and the potential for misuse.

• It is not clear whether the permissible discrimination under the Human Rights Act 1993 is proposed to be prevented – but if so, there are serious questions about whether secondary legislation should do so. The Code should not purport to restrict the use of information which is permissible under other (primary) legislation.

•Regarding sensitivity: are hashed signature-style encodings in templates or statistically digested information in tuned models still considered sensitive? In the absence of the templating algorithm, it is already nigh-impossible to reverse engineer anything meaningful from privacy-preserving templates.

•Blocking "inferring health information" would block solutions like detection of intoxication for vehicle operation, factory work, accessing controlled substances; as well as already existing forms of telemedicine, and remote sensing for pre-enrollment or eligibility diagnostics before the health Info Privacy Code kicks in.

•There is a difference between inferring levels of agitation in a person's voice versus monitoring call center audio loudness as measured in decibels to manage and escalate issues in call centers, but the

blanket suggestions would reduce all the public benefit. Furthermore, regulating biometric technologies which infer emotional state does not seem aligned with the OPC's intention to regulate privacy over biometric information for the purposes of identification, verification and categorisation. Emotional state does not inherently infer someone's identity or personal information and there are a number of positive use cases that infer emotional state for the benefit of the consumer.

Q13: What exceptions, if any, should apply to disallowed purposes?

DINZ Comment

If there are disallowed purposes, it's not clear on what basis the 'public benefit' of the exceptions has been assessed. For example, why the existing wider public benefits in the free flow of information seen elsewhere in the Act are not proposed to be included. In some instances research can be conducted without informed consent — subject to other controls.

Q14: Are there any other purposes you think should not be allowed?

DINZ Comment:

All purposes should be allowed in theory – but subject to the other requirements in the principles and in any potential Code, if a Code is developed..

COLLECTION FROM THE INDIVIDUAL CONCERNED

Q15: Do you agree with the proposal that some exceptions to IPP 2 would not apply to collection of biometric information covered by a code? If you think some exceptions that OPC proposes to remove should still apply, which ones and why?

Q16: Are there any other exceptions to IPP 2 that you think should not apply to collection of biometric information covered by a code?

DINZ Comment:

No to both Q15 and Q16. There will be instances where non-compliance is not reasonably practicable in the circumstances, or where it does not prejudice the interests of the individual. Assessing or enforcing compliance with such a standard would be impractical and unrealistic.

Q17: Do you agree with the proposed modification of the 'publicly available information' exception to respond to privacy concerns about web scraping?

DINZ Comment:

No. This limits the freedom of digital platform operators to decide how information on their platforms will be made available. If an individual consents to their information being made available in a form that permits web scraping (not that we support or accept screen-scraping as good practice given its potential for adding further fraud vectors), it is not clear why the law should prohibit this. It is not clear why the 'unfair means' principle is not sufficient — as it presumably is to prevent web scraping of other information.

Further, the assertion that people "would not reasonably expect their information to be used in this way" seems unfounded. We could equally contend that the typical member of society is more than aware of the risks of posting information about their real identity online because it could obviously be used by any agency or actor to identify or impersonate them. There is not a reasonable expectation by any partially-informed actor that biometric data they post onto social media or other web platforms remains their property or subject to their control.

The focus should be on preventing harm, rather than preventing activity. As described, Māori would be unable to collect publicly-available information about their own culture. Photos and recordings are not generally considered biometric information, so while these are privacy concerns they are not typically included in biometric regulation. Biometric analysis of publicly-available images only becomes a privacy issue if it is associated with an individual. It may be a cultural concern if distinguishing identity techniques are used - that would be a human rights issue such as discrimination.

Q18: Do you agree that there should be an exception to IPP 2 for collection of biometric information for testing or training automated biometric systems? If so, do you agree with OPC's proposed framing of the exception?

DINZ Comment:

No, but we appreciate the fine balance that needs to be struck here particularly with sensitive or confidential data.

Testing and tuning scenarios already fall under the "compliance is not reasonably practicable" clause, which we do not agree should be removed as an exception.

However, if some form of proposal for a code was to go ahead and that exception was not retained, then an exception for the procurement, development, testing, and training of an automated biometric system is generally appropriate. In essence, this should always remain a valid use-case in which explicit consent is not always mandated.

TRANSPARENCY

Q19: Do you agree that there should be additional transparency and notification requirements for biometric information covered by a code?

DINZ Comment:

It is difficult to offer a definitive Yes or No answer because the answer depends on the use case and the sector and the regulations covering that sector.

This section extends the exercise from focusing just on identification, verification and classification to any specific use of biometric information. If that is the purpose of this exercise then the definition of biometric information needs to be enhanced. There are many uses of biometric technologies that produce biometric information that is not relevant to an individual or is not even personal. The OPC is encroaching on other regulatory areas.

Passive collection of non-identifying biometrics would normally have notice rather than consent (e.g., “This is a hazardous area and is monitored. Do not enter without permission”). If someone enters, then biometric information may be essential to determine safety risk (e.g. "Is this someone authorised to be here?"). The way this is tackled overseas is that biometric information is not regarded as personal information until it is associated with an individual. At that point, or when the biometric data are collected actively from an individual, they are personal data but not private data. This is part of the reason why privacy and personal data protection are separated in other jurisdictions.

Q20: Do you agree with the specific proposed additional requirements with respect to:

- information that must be provided at the time of collection
- information that must be made publicly available
- information that must be notified to an individual at a later date?

DINZ Comment:

No. It is not clear how the additional notification requirements would provide greater awareness or higher levels of engagement. To do so would impose an administrative and compliance burden, as well as possible overcollection of contact details to comply, that outweighs the benefits, particularly the information that must be notified to individuals at a later date (without any indication of any reasonableness requirement for the period there would be significant impacts on the accuracy principle). It is not clear which information in a Privacy Impact Assessment is intended to be valuable, and noting that some of the information is often not required by law to be disclosed.

Q21: Are there any other ways in which you think that transparency can be improved?

DINZ Comment:

The consent and notification requirements already catch most of the transparency requirements, but for additional clarity passive vs active capture could be distinguished.

Informing the public where there is active capture and where other personal information is being collected at enrolment means an 'identity' is being captured in a database or data store and it is this information which make it particularly personal and sensitive, not an inadvertently captured photo without personal information associated, like CCTV footage, or in non-photo use cases like wastewater analysis seeking information about health or drug use where, alongside time-sampling and genomic sequencing and DNA analysis, it might (like the CCTV example) be possible to tie some aspects of the analysis to an individual, or a small group of individuals. In such passive-capture cases we recommend public signage or public education campaigns are important so that individuals are aware of where, when, and who may have inadvertently captured public biometric data.
Of course there are standing ISO and other internationally curated standards for de-identification with technology to support them.

Q22: Are there any other matters you think individuals should be informed about in relation to an agency's handling of their biometric information covered by a code?

DINZ Comment:

Informing customers where biometric information has been leaked or where biometric information has been misused by company staff is important. This includes setting good incident response mechanisms in place so that customers are informed proactively and without delay. Some members have indicated that with sensitive personal information they protect data at rest and in transit, enforce least-privilege access, enable logging and alerting, and create a Reportable Event Readiness (RER) incident response process for when information is leaked or otherwise compromised. These are difficult to mandate however, and could instead be best practices referred to in guidance.

Q23: Do you agree with the proposed changes to the exceptions to IPP 3?

DINZ Comment:

The rationale for removing the exception in IPP3 where individuals are not identifiable is not clear.

Testing these alongside the technology before formal adoption into a code or in guidance may serve to support that these are practical. In doing so, these measures will be balanced together with the additional transparency measures benefiting the public and individual and the benefits the particular biometric technology serves to the public and to individuals.

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

DINZ Comment:

PIAs could contain confidential internal information which is necessary to do the assessment justice. If a code required public disclosure of the specific details, then the purpose of the PIA is to communicate with the public, and much of the Privacy Impact Assessment would happen "outside" the PIA to preserve confidentiality, intellectual property, or national security considerations. Public disclosure of the performance of a PIA does not seem unreasonable, but necessitating those specific details be shared in a code does. In many cases, the Official Information Act (OIA) would provide ample means for public awareness of certain details if it were necessary.

CONSENT

Q25: Do you agree that agencies should be required to obtain consent before collecting an individual's biometric information covered by a code?

DINZ Comment:

No, we do not agree.

To do so fundamentally shifts the basis for processing of personal information under the Act – and it does not address the risk of individuals losing control of their biometric information. It is not clear who would 'consent' on behalf of children, young adults (presumably their representative?), missing persons, trafficked persons, and persons who need to be enrolled into a watchlist (i.e., they are not on a WL yet).

•If any such rule were to exist, a wide range of exceptions would have to be established to make compliance at all realistic. It may be more reasonable to suggest public disclosure that biometric information may be/is captured, but a requirement for informed consent is completely impractical in many use cases.

•It may be practical for certain sectors or use-cases to require informed consent and to provide reasonable alternatives when consent is not provided, which reinforces our suggestion of a more nuanced approach to this subject overall.

•This section again expands the reach of this exercise to any purpose, rather than just identification, verification, and classification. If this is to be a general personal data protection update to the legislation, then it is not a regulatory change. The definition for biometric information is broader than used overseas, which only makes privacy and personal data protection relevant if it is associated with an individual. They also clarify that recordings such as photos and audio are not biometric samples if they are not used for measuring physical characteristics. By sticking with biometric information the OPC may be unintentionally excluding personal information it should encompass.

Q26: Do you agree with the following specific proposals about obtaining consent?

- Consent must be express and specific: individuals must consent to each purpose for collection, and agencies must not rely on implied or 'opt out' consent.
- Consent must be voluntary, so individuals must be given an alternative to the collection of their biometric information where possible.
- Individuals must be able to withdraw consent to the collection of their biometric information.

DINZ Comment:

On the face of it, all three might seem reasonable, but the use-cases with biometrics can be complex when it comes to obtaining consent.

There are only three purposes being considered in this proposal: identification, verification, and classification. Other uses of biometric personal information might or might not justify these consents. These specific provisions have resulted in some punitive cases overseas that were harmful in other ways to businesses, customers, and the public. In one case it shut down online university exams for a country during COVID, as there was no alternative to webcam-based proctoring and one student complained. No actual privacy harm was quantified, only non-compliance with the rules. Please be careful with "Consent must be…" clauses.

If due diligence has been performed at the outset (per the code or some variant), then biometrics should not be being collected and used in an automated system without legitimate cause, in which case voluntary exemption would likely mean an overall worse outcome for the subject (requirement to collect even more personal information, slower service provision, higher likelihood of lower-quality management of them as an entity).

In addition to the university example above, there would be a wide range of use cases in which not having the data collected is not possible (e.g., where cameras cannot reasonably NOT capture one individual in an environment who does not consent), and mandatory adherence to allowing exception could significantly increase the complexity of administering any system.

Requiring post hoc revocation could introduce a wide range of complex requirements on agencies to administer identification that the claimant has sufficient rights to request withdrawal, which in of itself may create a circular loop of information being collected. This is especially problematic if the proposal for necessitating the deletion of raw samples were applied, as ownership or rights to decisions about templates would effectively be impossible to discern.

Q27: Should the individual be prompted at regular intervals to check whether they still consent to the collection of their biometric information?

DINZ Comment:

We assume here that by "collection" the OPC means retention of some previously-collected biometric (unless it is some continuous collection or ongoing authentication context)? If so, as with previous suggestions, a blanket requirement would not be feasible considering that some government agencies (and to a lesser extent some industries) require retention times measurable in decades, and the same agencies might manage millions of records, not all of which they have collected contact details for. Even if the follow-up re-consenting were only required infrequently (e.g., every 5-10 years), the scale of work may be enormous and disproportionate to any supposed benefit.

Existing provisions and existing expectations of the Privacy Act should apply equally well to all personal information, not only to personal biometric information. We note that some lower-sensitivity types of biometric personal information are much less likely to cause harm if compromised than some higher-sensitivity non-biometric personal information. Carving out separate Privacy Act expectations merely on the basis of whether personal information is biometric or non-biometric (rather than the contextual sensitivity of the personal information at hand) affords nothing by way of better protections to individuals.

Q28: If an agency is merged with or acquired by another agency, with the result that the agency holding biometric information covered by a code is different from the agency that originally collected it, should the agency that now holds the information be required to obtain consent in order to continue holding and using that information?

DINZ Comment:

Not if the purposes for use of the biometric information remain the same. Further, it would be extremely impractical and costly to execute engagement of this nature at scale if large holdings were transferred. As per Q27, the requirement would appear disproportionate to any benefit.

Q29: Do you agree with the proposed exceptions to a consent requirement?

- Where an exception to IPP 2 and IPP 3, as modified by a code, applies.
- Where collection is authorised under another law
- Where consent has been provided previously and not withdrawn.
- Where collection is necessary for the maintenance of the law.
- Where collection takes place within an employment relationship and is covered in an employment agreement.
- Where it is not reasonably practicable to obtain consent, and collection is necessary in relation to:
    - serious threats to health or safety
    - provision of health services
    - research relating to health or safety
    - watchlists of problem gamblers, or individuals who have been trespassed for violence, threats or criminal activity.

DINZ Comment:

Partially. Some exceptions appear narrower than the current law: e.g. the lack of reference to 'reasonable belief' in the maintenance of the law exception, without any policy justification.

Q31: Are there any other exceptions you think should be considered?

DINZ Comment:

For the prevention of serious threats to health or safety, it is not collection that should be the focus but the use. The exceptions to consent do not include other common grounds, e.g., to respond to a national emergency. The policy rationale for watchlists is not clear, and it appears to apply to only limited forms of (potential) harm. The focus on trespass notices conflates legal regimes and it is not clear how records of verbal trespass would be proposed to be demonstrated. Other harms are not covered (e.g., child sex offenders).

Many other exceptions should be considered: access to private spaces, non-identifying monitoring of public spaces, high-consequence health-and-safety environments or activities (not threats), non-identifying behavioural observation, and property protection.

SECURITY

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

What OPC is proposing

- **IPP 5** would be modified to provide for specific security safeguards that agencies would need to implement in relation to personal information they hold, if it is biometric information covered by a code. These safeguards would include:
    - Biometric information covered by a code would need to be stored (or, where relevant, transmitted) separately from associated biographical information.

DINZ Comment:

What is an actionable definition of "separate"? From a systems- and information-architecture perspective what does it mean to "store (biometrics and biographics) separately"? In measurable terms, what level of architectural abstraction, semantic differences, and physical location is far enough or separate enough?

This brings into play the expectations for different database tables, different servers or service platforms, different availability zones and different regions, and different jurisdictions. In many cases, business systems are purchased as whole concerns that will store biometric information in the same context as associated personal and biographical information (think of human-resources-management systems, student-information-management systems, systems used by hotel-and-accommodation providers, and the many systems designed explicitly for the purpose of capturing and managing biometric information about people.

That the determination of "separate" is so vague as to be unimplementable is a significant barrier. However, if biometric data are ever to be used and useful then agencies will require the ability to relink them and reassociate them with the personal biographical information of the individuals they represent. All of this makes "separate" storage and transmission of biometric data challenging to the point of being impossible. Any potential benefits of separation are achievable primarily by the adoption of good information security practices and by the application of good cybersecurity techniques, both of which are already expected by the Privacy Act and supported by the NZISM (see also the response below to Q32).

QUESTIONS

Q32: Do you agree that there should be more specific and heightened security requirements for biometric information covered by a code than the general requirements in IPP 5?

DINZ Comment

DINZ does not agree, particularly given how rapidly the technology and security environments are changing. Retaining the flexibility of the Act (one of its strongest points) is beneficial. Being more prescriptive runs the risk of being under-protective. We would instead suggest that existing recognised standards relating to data security should be included in the Guidance and strongly recommended. While it is appreciated what goal OPC is trying to achieve, ideally, deference should be given to an agency that has primary expertise in relevant security protocols and standards.

For example, remember that to secure systems, biometric templates are stored using zero-knowledge proof algorithms so there are no biometric data stored. As soon as zero-knowledge proofs are used, biometric technologies no longer collect biometric information.

Q34: Should a code (or guidance) cite specific security standards? If so, which ones?

DINZ Comment:

Yes. DINZ has given some examples above, but if expert consultation and co-creation were to take place, there are relevant ISO or other standards for security that could be referred to, but guidance should only come from credentialed sources. We also expect there should be sensible alignment with applicable NZ-created sector-focused standards and best practice; for example, the NZISM to the extent that it is up to date with international equivalents, and the identification management standards prepared by the Department of Internal Affairs that largely reflect applicable international standards and best practice, and which underpin the Digital Identity Services Trust Framework.

ACCURACY

Questions

Q35: Do you agree that agencies should be required to take appropriate steps to check the accuracy of the results produced by biometric systems?

DINZ Comment

Yes, accuracy is important, but no, an external compliance requirement is not needed. Is there any circumstance where a business wouldn't take steps to ensure their systems did what they needed them to do? An agency is harmed as well when their systems let them down. Arguably, the agency has more to lose from an inaccurate system.

We think there are several accuracy concepts conflated in this section, all of them meaningful and applicable in interpreting "accuracy of the results produced by biometric systems":

•the accuracy / quality of the raw sample ("is Bob's face clear enough to even template?," "did Bob upload his wife's photo with his own application?")

•the accuracy of the templating algorithm ("is that a face or just a pineapple on a Hawai'ian shirt?")

•the accuracy of the algorithmic solution producing some measure of similarity

•the accuracy of the threshold(s) the agency chooses to employ to bind the similarity measure into discrete outcomes ("match," "no match," "angry," "Bob Smith," "non-native speaker of English," "has high blood pressure")

•the accuracy of the agency's overall service decision ("deny credit," "issue passport," "allow access to the controlled-substance cabinet," "translate the instructions").

The last two bullets above are business decisions that control processing volume, cost, Failure to Enrol (FTE), timeliness, reputation, service-delivery friction, and, as such, should remain in the control of the business. The second and third bullets attempt to control technology, which is theoretically contrary to the OPC's intentions. The first one is already covered by the Privacy Act.

It may be reasonable to include in Guidance that agencies should not implement technological solutions that they cannot reasonably maintain over time proportionately to their use case. However, even if accuracy can be meaningfully and operationally defined, specific requirements may be overburdensome and result in denying the use of efficiency and privacy-enhancing technologies to smaller agencies that cannot shoulder the costs required to quantitatively assess this type of concept.

Q36: Do you agree with the specific accuracy requirements proposed by OPC? Are there any other accuracy requirements you would propose?

DINZ Comment:

No, we do not agree with the requirements proposed by OPC, particularly given how rapidly the technology environment is changing. Retaining the flexibility of the Act (one of its strongest points) is beneficial.

A bit more detail on our thinking on the concept of accuracy:

•input info accuracy vis a vis system matching accuracy vis a vis business decision accuracy;

•systems might need to be geared towards volume, FTE (or more specifically the Failure to Enrol Rate - FTER), timeliness, cost, introduced friction, and this is a business decision and not an empirical, scientific, or moral obligation

•differences between groups might be intentional and good, cf. positive discrimination or affirmative action

•equitable accuracy likely varies by situation: it's one thing for biometric assessment to declare a person is old enough to be admitted unchallenged to an R16 movie, another to waive the need for documentary evidence when purchasing alcohol, another to give somebody access to a bank account, and quite another to grant an individual access to a maximum-level-biological-safety research laboratory

•even biased biometric implementations could vastly outperform humans when it comes to neutrality, fairness, and consistency in assessments of biometric information

It should also be understood that for certain implementations an "accuracy" value of e.g., 99% may be considered exceptional performance, whilst in others that may be very poor performance. Dictating specific values or measures is not constructive.

Q37: Do you agree that the general accuracy requirements under IPP 8 are sufficient for the accuracy of biometric information used as inputs to biometric analysis, and for the accuracy of information used to decide to include an individual on a watchlist (where the watchlist involves detection of individuals through biometric matching)? Or should a code include specific accuracy requirements in these areas?

DINZ Comment:

Yes, the current requirements are sufficient, and any further specification veers into the territory of either regulating business decisions and needs, (national) security, or the technology and the standards. Specific accuracy requirements is wandering into the territory of standards rather than code of practice. If a standard is required, then the relevant industry should be setting it. For example the accuracy needed to identify someone needing special care will be different to someone who is dangerous.

Q38: Do you agree that agencies should be required to delete raw biometric information once templating of the information has been completed, or has failed, unless there is a good reason to retain the information?

DINZ Comment:

No. Deleting source samples would make identification and verification worse. The technology to generate templates is constantly improving, and without the source samples we can't make improvements. We would have to resample every time which would create a greater privacy intrusion and risk. A blanket requirement like this would harm many operators of biometrics technology.

The raw sample is near-uniformly necessary for good administration of any biometric system. Required cases include:

•in hybrid solutions that employ human assessors to verify, audit or disambiguate algorithmic outcome

•in forensic and investigative use cases that must maintain a chain of evidence

•if and when the agency updates or changes their templating or matching and classifying algorithm, the entire holding needs to be re-templated with the new templating algorithm and any vendor-specific matching algorithm, especially when the raw sample failed to template, so that any new templating mechanism can add it to the agency's holding

•as new methods emerge to detect presentation attacks like morphing and synthetic samples, the raw sample is likely richer in detail than the template

adherence to any accuracy principle proposed with require ground truth data to be able to be assessed against

Cybersecurity should be bolstered, not purposeless deletion. The known breaches are typically not by users of biometric technologies, but storers and aggregators of the information. Therefore, obliging the *users* to delete the raw samples is not achieving the intended goal.

Voice Recordings: We recommend that organisations keep the voice recordings that create a voice print or verification. We recommend as per the Australian and other jurisdiction requirements that the voice data and the biometric data be stored in separate encrypted files. The Voice data is important to be able to retrieve if a criminal process is started because of a voice match.

The typical chain of evidence for a conviction is;

1. Here is the original recording which created the voice print.

2. Here is the recording of the voice that matched the voice print.

3. An expert can attest to the voice biometric scoring and the likelihood that the Voice was a match

4. The accused person's voice can be compared and scored as part of the process

Other reasons to keep the recordings include recreating new voice prints if the voice biometric technology is changed.

Over and above these issues, organisations that have an obligation to keep records of customer conversations shouldnt be required to delete those recordings.

Images: Whilst it is possible to delete the original enrolled image of a person after making a metadata based face print and still use the FR system to detect enrolled people, deleting the enrolled image would be impractical in many instances because humans can't read metadata and need an image to look at on the screen to compare the enrolled person and the detected person's image.

Q39: Do you agree with the proposal that biometric information covered by a code must be deleted when no longer needed, and in any case retained for no longer than the notified retention period?

DINZ Comment:

As above — we do not think this would be practical. An absolute requirement of this nature would be unreasonable and impractical. Whilst the general principle of deleting information that is no longer required is sound, the notified retention period may have been incorrect, e.g., if retention beyond the notified period is subsequently required by law (including if a Privacy Act request is received on the day before disposal would otherwise be required) or other circumstances may now mean that retention is reasonable and lawful following the originally suggested period.

A specified retention period that must be adhered to runs the real risk of agencies specifying a longer period than would have otherwise been necessary to comply with potential legal requirements (e.g., an audit or investigation) and become an overall net-negative outcome for subjects.

Additionally, while it is relatively easy to delete a raw sample and the template of it, the biometric information used to tune an algorithmic solution is (in some microscopic ways) incorporated and "digested" into the matching algorithm, and "subtracting" it is not actually possible.

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

DINZ Comment:

The exceptions section may need strengthening from a crime-prevention perspective to enable organisations to create a voice print from recordings of someone that the organisation considers to be attempting fraud as well as creating a voice print from someone who has committed fraud. The Australian code or the Biometric Institute may be a good model for these exceptions.

It would depend on the level of granularity needed when it comes to specifying purpose vs directly-related purpose: is suspected fraud sufficiently directly related in purpose to investigations of known fraud? What if it is suspected identity fraud vs known insurance fraud or loan fraud, etc? How far apart will stop it being directly related?

Q43: Do you agree that it is the protections for biometric information in an overseas country that should be comparable under a modified IPP 12 in a code, rather than just general privacy protections?

Security over sensitive biometric information is an important consideration but this is important irrespective of where that data is stored. Therefore in reference to Q43, IPP 12 should be applied to all personal information equally – i.e., allowed to be stored in another jurisdiction with privacy rules

which are comparable to those in New Zealand. The OPC's own guidance on IPP12 clarifies that offshore cloud is not captured as 'disclosure' overseas[5]. Expanding this to have an exception for where it can only apply to jurisdictions comparable to those of the biometrics privacy code in New Zealand is impractical and would effectively introduce data localisation requirements which go beyond the Privacy Act 2020.

We believe modifying IPP 12 in this way would put New Zealand out of step with comparable privacy jurisdictions, and we suggest the OPC carefully review making such a requirement as this would limit, for example, New Zealand organisations using computing and storage capabilities offshore. Instead, we suggest the OPC focus on the importance of having strong security protections in place for *all* personal information, including biometric information. This suggested code of practice seems to have an underlying assumption that information can be accessed when stored offshore and that information will not be protected, but instead subject to offshore jurisdiction's biometric privacy rules many of which are nascent and early in development.

Q44: Do you have any other suggestions for modifications to limits on use or disclosure for biometric information covered by a code, including any new exceptions that might be required?

DINZ Comment:

Likely exceptions are needed for intelligence and security agencies in line with the policy that underpins the Privacy Act 2020.

Q46: If you are an agency that uses biometrics, how would our proposals affect your existing or planned uses? Would there be increased compliance costs, and if so, how could these be mitigated?

DINZ Comment:

Providing a detailed answer to this question would require a finalised set of proposed rules, standards, or other guidance that were to ultimately be brought forward. At a high level, it is likely that if some combination of the proposal were to be taken forward, costs of compliance would increase markedly: from fundamentally altering means of collection and ingestion of biometric data to increasing requirements for certain types of tuning or testing (impacts of which would likely apply to our vendors as well), to additionally collecting and maintaining previously not collected contact information to satisfy the notification and continuous / repeated consenting requirements. For agencies such as those at the border that can experience a much more dynamically-changing demographic of clients than purely domestic agencies, certain interpretations of some proposed clauses may require vastly increased costs of compliance (e.g., additional Data Scientists and testing environment implementations, etc.).

5 https://www.privacy.org.nz/assets/New-order/Your-responsibilities/Sending-information-overseas/1.-Principle-12-Guidance-web.pdf

A further suggestion concerns Grandparenting. Given that millions of New Zealanders have already enrolled their voice prints (e.g., with IRD) and any new code may change the consent or other data collection processes, perhaps those systems should be excluded from needing to comply with any new requirements for any existing users.

OTHER ISSUES

What other regulatory options could be considered?

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

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

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

GENERAL QUESTIONS

Q49: Do you have any suggestions for modifications that a code could make to IPPs 6, 7 or 13 in relation to biometric information covered by a code?

DINZ Comment:

As we have mentioned elsewhere and from the outset of consultation on this topic, guidance and voluntary standards is the best way forward, but only if they are co-created with industry.

Q50 (for Māori organisations or individuals): Do you have any suggestions about protections a code might include:

- specifically in relation to biometric information about Māori
- generally about biometric information, with impacts on Māori in mind?

DINZ Comment from Indigenous participant:

Create a separate Māori data privacy code or Māori information code that has legal effect, which safeguards the use of Māori data from a tikanga lens in many applications (specifically the issue of secondary use). The biometrics code, if decided upon, can then apply this.

DINZ Comment:

It is accepted that there may be challenges to overcome for this to take effect in active or passive biometric scenarios, particularly as this would potentially require first the need to identify a person in order to know that their data are Māori data and need to be handled according to a separate code? But given the great advancement of Māori data registers, etc, those authoritative sources could be used to help overcome such challenges.

Q52: Overall, do the proposals in this paper strike the right balance between flexibility and technological neutrality, and clarity and certainty for regulated agencies?

DINZ Comment:

Not really because they are obfuscated by lack of clarity and by scope-creep in some areas. There is inconsistency between the focus on Identification, Verification and Classification in the scope of the Code and the IPP proposed changes that relate to "any purpose". This is confusing. The language jumps between "someone" and "individual" which also have different meanings. There is overlap with other regulations, and subjects outside the scope of protecting the privacy of the individual. While the goal and intent to address concerns is great, there is room for improvement around clarity and certainty.

Q54: Are there any ways in which our proposals could have unintended consequences? If so, please let us know what these are and how they could be addressed.

DINZ Comment

Biometrics is an area that can dramatically improve privacy for everyone: reducing privacy risks; reducing the cost and effort to manage digital identities; and even enabling greater cultural respect and recognition. One likely unintended consequence of setting a code of practice is that early adoption of biometrics will be hampered. There is no concept of privacy enhancing — making things better than they are today. Instead, there is an ideal practice defined in a code.

We'll mostly have to wait until the rest of the world has reached that ideal because compliance will be onerous or too risky in New Zealand. In the meantime, we stay on less-private systems and don't develop the expertise that could improve our privacy stance. Building guidelines together until we reach a stage when a code of practice is viable would yield better privacy outcomes.

The proposals for a code could suspend, reduce, or delay use of biometric information, to the detriment of information security and customer service. The proposals could also stunt development and innovation that would in time improve the accuracy and acceptability of less well known / trusted use cases. By addressing concerns of some parties, the privacy-enhancing and the privacy-preserving benefits to others may be reduced or delayed significantly, and we might also miss positive discrimination opportunities.

Accepting that the OPC is concerned with the scope and function creep of biometric information (and technology), these proposals from the OPC actually exhibit scope-creep themselves — out of the privacy field and veer into a range of primary legislation potentially leading to collisions; for example:

– security related Acts like Policing Act, Immigration Act, Customs and Excise Act, Intelligence & Security Act

– Controller and Auditor-General's mandate, Digital Identity Services Trust Framework Act, Human Rights Act, Unsolicited Electronic Messages Act, Fair Trading Act, Employment Relations Act, Harmful Digital Communications Act,

– international standards in records management, digital identity, biometrics, and cybersecurity,

– intellectual property law, and a host of technology and innovation fields

This scope-creep can be avoided by the following agencies co-creating and co-developing the guidance with OPC: MBIE's Standards NZ and Cert NZ, ISO participants in New Zealand of the relevant ISO standards, Digital Identity New Zealand (DINZ), Cross-Government Biometrics Group (CGBG), technology vendors, etc.

Given the size of Aotearoa and the extremely high expertise needed in this field, recruiting, developing, and retaining subject matter experts is already difficult. As the number of public and private sector agencies needing advice, guidance, and oversight increases, a central government agency uniting experts might be needed. This sort of Centre of Excellence (or alternatively Aotearoa appoints a Biometrics Commissioner) would reduce the risk of scope-creep by aggregating knowledge, developing experts, and serving all agencies with their bespoke technological, technical, algorithmic, policy, ethical, reporting, testing, tuning, thresholding, de-biasing, and Algorithm Charter compliance needs.

Q55: Can you suggest alternatives to any of our proposals – ways of achieving the same or similar outcomes by making different modifications to the privacy principles? If so, why would these alternative proposals work better?

DINZ Comment:

Guidance and expectation-setting, with a period of active regulation, in advance or instead of issuing of a code.

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

DINZ Comment:

DINZ has made its point multiple times so it needs no repetition here. Guidance and standards are tools that should be used here.

Q57: Do you have any other comments or suggestions?

DINZ Comment

The document doesn't cover anonymised use cases because those don't use biometric information; e.g., people-counting, anonymous demographics (age, gender), even potentially-anonymous *memory* of people potentially for either identifying and statistically-reporting for communities or actually providing some kind of soft or digital intervention from a health, safety, and wellbeing perspective in situations involving risky behaviours like gambling or alcohol or not wearing a helmet while riding a bicycle), traffic flows etc, where anonymous data might be used for site or store traffic planning and layouts.

For instance, a retail mall may want to know where choke points are on certain days and times, or when there are more older women etc in a store or area at a particular time. These use-cases don't actually identify anyone specifically, nor do they enroll anyone's biometric information in the system, so they shouldn't be caught by the specific restriction on marketing. It must be made clear that this is an acceptable use of Biometrics. Unclear understanding leading to unclear wording will result in unintended restrictions on the use of the technology.

As it stands, it's hard to intuit the intention behind many of the definitions and concepts that look straightforward theoretically, but are operationally very complex as we have pointed out above. Some examples:

• "accuracy": accuracy of input data vs accuracy of algorithmic solution vs accuracy of thresholds vs accuracy of agency's business decisions

•what is a sector-agnostic definition of "necessity and proportionality" for biometric information collection?

•what does it mean to "store (biometrics and biographics) separately" as we stated in our response to Security above Q32. Why and how far is separate enough?, different tables, different servers, different jurisdictions?.

•what is "independent" testing? Independent of whom / what? Of clients, users, vendors, production data?

•given obligations / cyber architecture around backups, cloud architecture, auditing obligations, and data sharing agreements, what does it mean to "delete" something?

•the difference between "biometric information" vs other personal information, noting that at a large enough scale most everything becomes identifying (your old COVID tracer app and your current GPS are behavioural biometrics)

•information vs technology: not as discrete as we'd like to think, noting that a tuned machine learning model is straddling this divide perfectly

•“surveillance”: Biometric technology is not sentient: As we pointed out in our response in 2022, people and intention to surveil are the causes of surveillance, tracking and profiling, not biometrics. This is a concern about the use of technology, and not about the technology or the magnitude of the collected data itself. Additionally noting other legal frameworks relevant here, there is the further consideration that all three processes (surveillance, tracking and profiling) may be lawful and supportive of national security if done responsibly.

Biometric templates are algorithm-specific and not human-readable. The fact that they are not identifiable outside of the internal components of one particular solution with a mated biographic record needs to be considered because it raises the legal-philosophical question whether something that is ordinarily not perceived as personal information satisfies the requirements of being personal information. An inaccessible x-vector template of someone’s voice is of and “about” an individual, but if it is unreadable, un-processable, un-reverse-engineerable, what privacy risk does it represent in practice?

To reconcile the abstract objectives with operational practice, kaitiaki in this space will need to at least entertain the idea of some consensus Key Performance Indicators that can be both measured and improved on, as a direct result of the intervention (be it guidance or a code).

Public understanding of the technology also needs to be vastly improved to dispel stubborn myths or misinformation that have been intentionally circulated in partisan media, often based on research that was either based on ground truth errors or has been vastly improved upon since. Conversely, we observe that the millions of New Zealand citizens who have obtained passports and access to services over the years, the tens of thousands of call-centre interactions daily, the millions of travellers annually whose journeys were facilitated, or the prevented harm and improved national security measures eschew media attention — despite biometric solutions being at the core of many of them.

The proposals for a code with regulatory ‘teeth’ simply do not have the same level of flexibility as the Privacy Act itself, and as such it becomes dated very quickly given the rate of development in the space. With Guidance, updates due to technological advancements are much easier to convey and act upon. This is not the case with regulation which has a slower reaction time.

Changing many moving parts at the same time could create problems, even if each individual change looks sensible and operationally feasible otherwise. For example, requiring both the raw samples destroyed and a subject's ability to request the removal of their remaining biometric template means that the agency would need the requestor to submit a new biometric sample so the agency can search for, find and remove the original template! Otherwise the agency couldn't ensure that the requestor is in fact requesting the removal of their own records.

Addendum

New Zealand

A high level analysis of Personal Data Protection and Biometric Definitions

14 August 2023

Background

The Office of the Privacy Commissioner (OPC) is asking for feedback on possible new rules about biometric information. OPC is thinking about whether there should be a set of rules called a code of practice. A code could change how the privacy principles in the Privacy Act apply when organisations use technology to analyse biometric information.

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

Further information is available here:
https://www.privacy.org.nz/publications/guidance-resources/biometrics-and-privacy/

Key Findings

- The only uses for Biometric Technologies that have been regulated overseas (in liberal democracies) for privacy are:
    - **Identification**
    - **Verification**
    - **Association**: There are scenarios where biometric information gets associated with a uniquely identifiable individual. At that moment it becomes part of the personal data for that individual. Until that point, the use of biometric technology is not generally considered as in scope for privacy regulation.
- Where the collection of biometric information is not associated with an individual, it is generally not considered personal information of an individual, and privacy principles are unlikely to apply. However, privacy principles are also good data management principles. Any collection of biometric information is likely to have the equivalent confidentiality principles applied.
    - Biometric information that has been collected as personal data for an individual cannot be repurposed without consent. If an individual consents to their data being anonymised to use for other purposes, the disassociated biometric data is not personal data. The original personal data linked to their identity remains as personal data and retains full privacy protections.

- Human rights, safety, policing, child protection, and other legislation may apply depending on how biometric technology is used. For example, discrimination is a human rights concern, it is not a privacy concern.
- There is over two decades of global research into the regulatory concerns described by the OPC. The European region has been leading these initiatives globally. The Article 29 Working Group assembled a significant body of knowledge that informed the European GDPR legislation.

- Using personal information in marketing activity is well established, as is the application of privacy regulations to this activity. Biometric information potentially extends the reach of **automated marketing processes** from electronic communications into the physical world but does not change how marketing activities consider privacy. Same rules, different tools.
  - Using biometric information to target direct communications with someone would be equivalent to using an email or phone number in direct marketing. The Unsolicited Electronic Messages Act should cover this but may need updating.
  - Using biometric technologies in direct selling may be relevant to the uninvited direct selling provisions of the Fair Trading Act. These provisions may need updating, as the place and type of uninvited direct selling may be out of date with newer technologies.
- The definitions globally have not been developed to sufficiently differentiate between the different types of biometrics relevant to privacy. With practical adjectives we can encompass current and future technologies without being technology specific. The following are proposed:
  - Methods:
    - **Observable**: can be sampled or measured externally
    - **Evidential**: Requires the testing of a biological sample
  - Presentation
    - **Public**: biometrics are presented by the individual to the world as part of their participation in society.
    - **Private**: biometrics can only be measured if the individual provides personal access.
  - Examples: facial recognition is publicly observable, blood test is privately evidential, a fingerprint/retina scan is privately observable, alcohol detection in breath is publicly evidential
- There are important distinctions between intended **use, misuse, and abuse** of technologies. Outright banning of intended uses is appropriate if there is a likelihood of consequential harm from that intended use. If misuse can result in harm, then policies and practices to mitigate risks and minimise incidents are appropriate. If abuse is likely, then risk avoidance or elimination strategies are required.
  - There are many use cases where biometric technologies can avoid or eliminate the abuse risks inherent in legacy identification technologies. A code of practice should apply the appropriate controls. For example: do not ban something good because it might be misused. Instead, use appropriate controls to reduce the risk.
  - Because publicly observable physical characteristics are specific to a person, the relevant biometrics are inherently more secure than digital identification issued by a 3rd party. Biometrics enables portability for individuals. Their identity can move to new systems or providers in the event of a privacy breach.

- A **code of practice** carries the same legal weight as the legislation in the privacy act. There are many unknowns and assumptions which would make legal requirements difficult to articulate or comply with. Alternatives, such as an industry body charter, issuing guidelines, or standards accreditation may be effective alternatives to address public concerns. These should have greater consideration before settling on a code of practice.
- Jurisdiction may be challenging, as most businesses that use biometric technologies will outsource the application to a service provider. That service provider is likely to be headquartered in another jurisdiction, along with hosting the services. Data Protection regulations established overseas define the role of the **Processor** or **Controller** and describe how to handle cross border considerations.

Relevant Terminology

- **Data Protection**
  - The legislative structure used in places like Europe focus on Data Protection as an activity rather than social concerns such as harm, privacy, or discrimination. Consequently, in NZ data protection is distributed across different agencies: MBIE is concerned with customer data, DIA has digital identity, Justice has Digital Harm, OPC has privacy, Human Rights Commission has discrimination, etc.
  - Overseas focus on Data Protection allows them to narrow the focus onto the specific activity and allow the socially focused agencies to leverage as appropriate. That way misuse or abuse of biometrics can be specific to the social laws, and proper management/governance of personal data can be regulated as a compliance to good practice.
- **Data Subject**
  - Rather than individual, the term settled on is Data Subject to describe the person who is the subject of biometric data. This resolves a lot of issues where the data subject is not known until the biometric information about them is processed to determine identity.
- Methods:
  - **Active** collection – requires the data subject to actively engage in the process of collecting the biometric information. E.g. Fingerprint scan
  - **Passive** collection – can be collected without the data subject being aware. E.g. Facial recognition.
- Information Types: Rather than public and private
  - **Universal**: a characteristic that all people have
  - **Unique**: a characteristic that is unique to each person.
- Storage: There is a (mistaken) assumption that collection always results in permanent storage.
  - **In memory** – data is only stored during processing, and then discarded.
  - **Decentralised** – information is stored either by the data subject, or 3rd party.
  - **Centralised** – data is stored by the organization that is relying on it for identification.
- **Traces**:
  - Biological samples left behind that can be used to collect biometric data – eg fingerprints, DNA, bodily excretions.

- **Zero-Knowledge Proof**
    - This is a major technology advance since the data protection work done prior to 2010. This enables decentralised identity and verification without any exchange or retained knowledge of biometric information.
- **Privacy-Enhancing Technologies**
    - Rather than view everything as a threat, many of these technological advances have the potential to enhance privacy. The OPC paper calls out support for innovation, but only views advances through a risk lens. There is no support or recognition of efforts to pursue privacy enhancement.

References

- IAPP - https://iapp.org/news/
- Article 29 Working Group – WP 80 – Working group on Biometrics: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf
- Office of Victorian Information Commissioner: https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/
- GDPR Controller/Processor: https://gdpr-info.eu/chapter-4/
- GDPR cross border: https://gdpr-info.eu/chapter-5/
- EDPB – USA adequacy decision 10 July 23: https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf
- IAPP, EU Data Services Act: https://iapp.org/media/pdf/resource_center/digital-services-act-101-chart.pdf
- IAPP, EU Data governance act: https://iapp.org/media/pdf/resource_center/data-governance-act-101-chart.pdf
- Anonymity Terminology proposal: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf
- Comprehensive peer review of Article 29 Working Group; https://link.springer.com/chapter/10.1007/978-94-007-7522-0_3
- Changing Perceptions of Biometrics Technologies; https://www.aic.gov.au/sites/default/files/2021-05/rr20_changing_perceptions_of_biometric_technologies.pdf

The following Annex has been deliberately retained from OPC's Consultation released 25th July 2023 to assist later reading and contextualisation of DINZ's comments to it in September 2023.

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

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

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

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

Employment

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

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

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

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

Retail

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

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

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

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

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

Gambling venue

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

Under the proposals, the venue must show the use of live FRT to identify excluded persons is a lawful and necessary use of FRT in light of benefits and risks (modified IPP 1). It is likely the requirement for lawful and necessary collection is met, given the existing statutory obligations of gambling venues around harm minimisation and requirements to monitor problem gamblers.

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

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

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

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

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

Airports

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

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

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

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

Law enforcement

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

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

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

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

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

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

Financial / legal

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

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

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

Personal device

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

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

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

Targeted advertising

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

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

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

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