SUBMISSION BY

DIGITAL IDENTITY.NZ

to

OFFICE OF THE PRIVACY COMMISSIONER

on

DRAFT BIOMETRIC PROCESSING PRIVACY CODE

March 2025

Prepared by the cross-industry Biometrics Special Interest Group of Digital Identity NZ (DINZ) with input from individual subject matter experts as well as DINZ member organisation representatives from a mix of large / medium corporates, public service agencies and academia.

Digital Identity New Zealand thanks the Office of the Privacy Commissioner (OPC) for the opportunity to provide a submission.

DINZ authorises OPC to release its submission. Please also note that DINZ will also be publishing its submission on the DINZ website.

As always, we are happy to provide any clarifications in writing, on a call, or in a physical meeting.

DocuSigned by:
Colin Wallis
F84DA1755B8C410...

Colin Wallis
Executive Director,
Digital Identity NZ
M +64 21 961955 Wellington

About DINZ

DINZ is a not for profit, membership funded association and a member of the New Zealand Tech Alliance. DINZ is an inclusive organisation bringing together members 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, inclusive Digital Identity ecosystem for Aotearoa New Zealand that enhances Kāwanatanga (honourable governance), Rangatiratanga (self-determination and agency) and Ōritetanga (equity and partnerships).

DINZ continues to lead efforts in advancing the understanding and responsible use of biometrics for identity within New Zealand. By focusing on education, dialogue, and input from biometric specialists (this submission is such an example), DINZ aims to enhance trust and efficiency in identity systems. Alongside education, DINZ is spearheading the development of a face image dataset that represents the population of Aotearoa and is managed to meet public concerns, subject to sponsor support. It will be a world-first, country-specific dataset if DINZ can pull it off. Face images are an extremely important biometric in the identity space as they are the sole biometric that has a verified image held by a government agency. Through these initiatives, DINZ is setting a foundation for a secure and inclusive identity ecosystem.

Previous Feedback

DINZ has previously submitted that a Biometrics Code of Practice is unnecessary (at least at the outset), will stifle innovation, and requires technological and specialist practice experience and expertise that OPC is not widely known to possess. We believe that in the case of this Code, the Code operates beyond the OPC's mandate. The Privacy Act 2020 is more than capable in providing the necessary guardrails when implementing biometrics provided that it is accompanied by clear guidance that is co-created by subject matter expert implementers with real world operational experience.

Introductory remarks

The primary goal for OPC as a regulatory authority is to prevent harm to individuals from the use, misuse, or abuse of their personal information. The Privacy Act does not define a regulated industry; it defines principles that businesses should apply to prevent harm to individuals. OPC has introduced Codes of Practice to help apply these privacy principles to regulated industries, so there is alignment between industry compliance and privacy protection obligations.

The use of biometric technologies is not specific to any one industry, and there is no compliance-based regulator for OPC to align with for this Code of Practice. This is at the heart of the challenge OPC has faced in forming a code specific to the use of biometric information. In the absence of a specific industry, OPC needed to define a space where this code applies, and where it doesn't. OPC then needed to define specific activities by specific people so the code can be applied to the processes of concern. We believe that the proposed code does not adequately meet these requirements. The consequence is ambiguity and heightened risk aversion. The sad irony for all of us

striving for better privacy outcomes is that biometric technologies can provide better privacy outcomes, but the code will potentially be an obstacle to investment in better privacy.

The lack of a specific industry is expected to be also the central challenge we foresee OPC facing when the Code comes into force. For the other codes, there are industry standards, rules, and regulations because there is a distinct industry.

As highly accomplished privacy specialists OPC has made an impressive effort to respond the public concerns about the possible harm from businesses using, storing, and collecting personal biometric information when deep subject matter expertise alongside extensive implementation and deployment experience of biometrics is not at the core of its 'raison d'etre'. There are some excellent guidelines contained in the Code and supporting material, which from the outset, is why we have supported the OPC issuing guidelines rather than establishing a code of practice.

An example of the importance of subject matter expertise: The Human Rights Commission consultation document refers to the immutability of faces and other biometric information. This enables biometrics to enhance privacy, while also creating a potential for a new form of identity theft.

DINZ still remains concerned regarding the biometrics-specific definitions. At this advanced stage of the process we should not be questioning definitions. In part, perhaps this is due to the code drafters using the same terms used for example by international and national standards bodies (whether by design or by accident) and giving a different nuance to meaning, remembering also that the meaning emanating from those terms had particular implementations in mind in the context of the standard in which they appear. Not only does it give rise to the potential for local and international confusion for biometrics implementers and deployers, but in some cases also may also put us collectively on a possible collision path with standards development organisations where those terms are used. If the code is not to follow international standards or those of comparable jurisdictions, then ideally the code should avoid using the terms contained in them and replace them with a term not used, or at the very least notate them 'adapted from'.

DINZ's current position regarding the code

Overall, the changes OPC has recently undertaken have without doubt improved the code. However, we continue to have concerns around definitions and scope, and some concerns in aspects of the proposed implementation which are set out below with constructive recommendations to remediate where possible.

We strongly recommend OPC looks to set a cadence of collaborative co-creative engagement with biometrics subject matter expert implementers and operational deployers, and schedule updates to the guidance semi-regularly and institute a 1-2 year review on the regulation itself based on how it's being used in practice. The time-honoured approach to consultation in Aotearoa whereby the responsible agency drafts something and releases it for comment in multiple rounds is not fit for purpose in continuously evolving, technically complex areas that require a rare mix of deep subject matter expertise combined with extensive practical implementation and deployment experience, such as bit exclusive to biometrics. If the legislation, structures and processes of the 'Machinery of Government' need to change, so be it. As a nation, we can and must do better.

DINZ exists for and because of its members. Accordingly, it will endeavour to establish a programme to inform and educate its members on how to confidently implement biometrics, in order to restore proactive interest in and inspiration for biometrics so that members can lead the charge - very much in the way DINZ has gone about informing and educating its members on the DISTF and DISTF accreditation, and might do in the near future on the CDP/CDR regulation.

DINZ would like to learn more about how this proposed biometrics code is intended to be implemented in practice, in particular how things like proportionality assessments would be reviewed in retrospect by the Privacy Commissioner. Should an agency for instance, who had no intention to cause harm, have conducted a full privacy impact assessment and assessed that on reasonable grounds that the biometric processing is proportionate to the likely impacts on individuals (rule 1(c)) ahead of applying the technology, how would the Privacy Commissioner have determined whether this was proportionate and reasonable in retrospect.

DINZ Specific Feedback

Definitions

Below, please find an itemised list of concerns regarding definitions and their impact on the Rules.

Biometric characteristic

“To be within the scope of the proposed code, biometric information must meet all of the following criteria:

1) the information must be personal information; 2) it must be about a biometric characteristic; and 3) the collection or use of the information must be for the purposes of biometric processing involving either biometric identification, biometric verification or biometric categorisation”.

Under the second limb of the test, personal information must be about a “biometric characteristic”, which is defined as:

(a) a physical feature or quality of any part of an individual’s body including their face, fingerprints, palmprints, iris, retina, voice or vein patterns; or

(b) the way that an individual typically performs or responds to a task, action or decision with any part of their body, whether voluntarily or involuntarily, including the repeated motion or associated rhythmic timing or pressure of any part or feature of an individual’s body such as the individual’s gestures, gait, voice, heartbeat, eye movements, keystroke pattern, signature or handwriting style; or

(c) a combination of any such distinctive attributes, including the way an individual sounds when they speak.

This definition is very broad, and goes beyond similar definitions in other jurisdictions. For example, in the US, “biometric data” is usually defined as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. The proposed definition under the draft code, by contrast, includes many measurements that are not

biologically unique to an individual, which would put the New Zealand approach out of step with other jurisdictions.

Biometric sample

A "biometric sample" is defined as "an analogue or digital record of an individual's biometric characteristic". As currently drafted, as a literal interpretation, a "biometric sample" may include mere photographs, videos or audio recordings, where those photographs, videos or audio recordings relate to an individual's biometric characteristic. Notwithstanding this, in most parts of the draft code, the definition of "biometric sample" is relevant only by virtue of its inclusion in the definition of "biometric information", where it is qualified by a requirement for biometric processing.

While we understand the intention of the draft code is to capture biometric information as it relates to a biometric characteristic used for the purposes of biometric processing, we note the requirements under Rule 2 apply to "biometric sample" rather than "biometric information" (with the latter incorporating the concept of biometric processing). We assume this is not intentional, and is contrary to the intended scope of the draft code as set out in the Commissioner's guidance (see p. 6). In light of this, we recommend Rule 2 is amended so that it clearly applies *only to collection of a biometric sample "for the purposes of biometric processing"*.

Veins, arteries and blood are considered specialized connective *tissues*, so currently meet the definition of "biological material" in the code. As a result, vascular biometric samples (finger, palm, and wrist vein, as well as retina and sclera based approaches), and biometric preprocessing steps to normalize over blood-pressure effects in image processing are possibly not (or only ambiguously) covered by the definitions of "biometric information" or "biometric characteristic". Foreseeably, biometric processing (whether for identification, verification, classification or liveness detection) will keep running into the fuzzy boundary between "biological material" and "biometric information" - infrared, hyperspectral and thermal imaging both as preprocessing steps and feature extraction steps - will need to negotiate what to do with blood pressure and body temperature per body landmark, as examples.

Template vis a vis Feature (set)

While DINZ fully supports the OPC using ISO standard definitions, **if** the Code will not use ISO standards, the current distinction between a "template" and a "feature (set)" is possibly superfluous: 1) a biometric feature (set) becomes a template when it is stored for reference, 2) in the Code so far, feature only serves as some indistinct version of a template, never really meaningfully distinguished from the template.

Biometric Result

DINZ is unsure if the definition of "biometric result" was meant to be comprehensive, but "candidate list" or "gallery" is still missing in (a). "Undetermined" and "inconclusive" should be moved to under (b) in the definition, as those are comparison decisions, just like "match" and "non-match". To stay in line with the ISO standard definitions, we would recommend removing 'positive' from match in (b). It's important to note that biometric comparison (whether it's 1:1 or 1:N) will strictly output nothing but probe-candidate similarity measure(s), or some likelihood measure that the probe is in a certain category. An alert, a granting / licencing / authorizing decision, a recommendation, an inference, but even a match or non-match comparison outcome or a classification label based on thresholds are **business decisions** and not resulting directly from "biometric processing". So if the definition of "biometric result" is supposed to reference the **direct** outcome of "biometric processing" (as

opposed to other business decision processes far, far downstream from biometric processing), a large number of the list is irrelevant in the definition.

Biometric Verification and Biometric Identification

The definitions of "biometric verification" and "biometric identification" are still circular and misleading, not to mention not in line with ISO standards and / or comparable jurisdictions.

The definition of "biometric verification" is currently not only circular (verification means verification) but also includes "authentication" which ISO specifically advises against. We still recommend following ISO standard definitions and distinctions and avoiding merging them in an ad hoc manner. Additionally, you cannot store anything in a "biometric system", given that its current definition (both in the draft code and by ISO) is only a processing unit / engine. We suggest the ISO standard definition of a biometric database (37.03.07), and biometric enrolment database (37.03.09) vs biometric reference database (37.03.17) in ISO/EIC 2382-37:2022. Furthermore, the current definition of "biometric verification" makes the incorrect assumption that during verification anything verified applies to the "identity of the individual". Biometric verification is only confirming a biometric claim (i.e., does this feature set look sufficiently similar to this template to assume that they both originate from the same biometric capture subject) – even in the absence of linked raw sample or any biographic information like name, DoB, driver's licence or passport number. This distinction is materially crucial in an operating system.

Regarding the definition of "biometric identification", DINZ recommends avoiding yet another commonly misunderstood concept, "recognition". The ISO/IEC 2382:37-2022 definition uses recognition as a cover term for both verification and identification, i.e. as a synonym of biometrics itself! As mentioned in the previous paragraph, the current definition of a "biometric system" (both in ISO and the code) is basically that of the processing engine (be it fully algorithmic, or hybrid human-augmented-algorithmic), but does not include the biometric template holdings of the processing agency. DINZ encourages the introduction of the ISO definitions 37.03.16 biometric reference and 37.03.17 biometric reference database to specially carve out holdings that are attributed to a natural person, vs. 37.03.07 biometric database (a database of biometric data not attributable to biometric data subjects). For clarity, biometric identification by ISO's standard only searches against a biometric enrolment database to find and return the biometric reference identifier attributable to a single individual (if any is available in the database above a certain match score). The OPC's definition ("establishing the identity of an individual") assumes the additional steps of the reference identifiers being linked to a **biographic** database, and retrieving the associated **biographic** details like name, DoB, etc. These differences matter materially in operations: as an example, a search against a face-only watchlist (where the agency does not have biographic records for the enrolled capture subjects) would not meet the current definition of "biometric identification" in the code, but it is certainly meeting the definition of biometric identification in the ISO standard ISO/IEC 2382:37-2022.

Readily Apparent Expression

The interpretation of "readily apparent expression" is far from trivial or low risk. It is not trivial for an assessor to decide if a person with Parkinson's disease just nodded in consent or whether the assessor is witnessing tremors in the neck muscle. Similarly, offenders' interpretation of victims' expressions, like smiles, are regularly contested in court in hundreds if not thousands of sexual assault cases. Audio volume / amplitude changes are also not trivial to interpret in a noisy context, so whether humans or machines make these judgements in a hybrid system about readily apparent

expressions, the code / guidance should cover these use cases in detail because the potential to harm exists.

Accessibility

The definition of 'accessibility' is of concern to DINZ. (Note that we raise it here under definitions for easier review, but also below under our comments regarding Rule 10). Rule 10(7)(a) considers "accessibility", but the current definition of accessibility does not consider that even in the absence of a disability, accessibility is desirable: non-native speakers of a target language are not disabled but could benefit from an audio signal processing algorithm that sorts them into native(-like) vs non-native speaker categories to facilitate access to translators, interpreters, or more readable documents. Or people wearing different types of footwear might pose different tripping, slipping, and catching hazards (for example on an escalator or construction site).

Individuals, for whatever reason, might want to know where they place on various continua along the categories of personality, mood, emotion, etc., but Rule 10(5)(b) seems to prevent them from consenting to and contracting such services?

Responsible and ethical implementation

As noted in the consultation document, biometrics have a range of beneficial uses, and the intention of the draft code is to ensure there are systems in place for organisations deploying biometric systems, particularly high-risk uses of biometrics. DINZ generally supports the use of biometric technologies, recognising their potential benefits in terms of convenience, efficiency, and security. However, DINZ emphasises that the focus should be on the responsible and ethical implementation of these technologies.

Rules

Rule 1

The case study examples provided in the Commissioner's guidance demonstrate that organisations must assess the benefits and risks before deploying biometric systems. In light of this, we recommend an amendment to the necessity test under Rule 1(b) to provide more room for the agency's reasonable judgment. Specifically, we recommend *the inclusion of the underlined text*, which reflects the current wording of Rule 1(c):

Rule 1 - Purpose of collection of biometric information

(1) Biometric information must not be collected by an agency unless, in the particular circumstances —

(a) biometric processing is for a lawful purpose connected with a function or an activity of the agency; and

(b) t<u>he agency believes, on reasonable grounds that</u> biometric processing is necessary for that particular purpose, including -

(i) that biometric processing is effective in achieving the agency's lawful purpose; and

(ii) that the agency's lawful purpose cannot reasonably be achieved by an alternative means that has less privacy risk; and

(c) the agency believes, on reasonable grounds that the biometric processing is proportionate to the likely impacts on individuals; and

(d) the agency has adopted and implemented such privacy safeguards as are reasonable in the circumstances.

This amendment would ensure that Rule 1 is applied in a way that allows organisations to take into account the relative costs and benefits of biometric approaches versus other alternatives in a proportionate manner.

DINZ agrees that organizations should examine the effectiveness of solutions. However, effectiveness is different from proving that the solution is effective. The requirement that biometric processing should be "effective" makes it look like that it is a binary attribute (something is either effective or not, with nothing in between), and as a result the regulator seemingly cannot accept gains in effectiveness. Agencies' demonstration of improvement over the already existing solution or alternative solutions could be deemed sufficient.

Given the privacy risk elements associated with this rule, DINZ notes that what is missing from the requirements around privacy risk is the explicit consideration of already existing privacy risk in current state solutions, which are often based on purely biographical identity management, or human-only processes.

Further feedback on Guidance for Rule 1

On pp. 46-7 the safeguards suggest "If the bias could lead to discrimination, you should not use the system unless the bias can be sufficiently mitigated to a level that no longer carries a significant risk of discrimination.": This suggestion on one hand rules out trying to net efficiency gains in processing, ignores the predictably stubborn, microscopic biases that might persist even in top-of-the-shelf solutions (1 error in 1M faces from group X vs 1 error in 2M faces in group Y), and ignores the operational fact that however biased the incoming system may be it might actually be a vast improvement over current-state human decision making in terms of fairness, neutrality, speed and consistency.

The testing scenarios on p. 46 are useful, but given that the code is now considering hybrid systems as well as fully automated systems, OPC should consider adding the aptitude testing, benchmarking, error monitoring and auditing of *staff* involved in these systems. Training staff is certainly needed, but research evidence shows it is not enough when employing human assessors to compare images. Assessors need to display an extremely high level of natural aptitude in this domain, so we recommend aptitude testing in personnel selection, training and ongoing benchmarking staff as the bare minimum requirements here.

This section in the guidance also introduces the terms 'references' (as well as 'database') which are not defined anywhere yet. The terms 'small', 'medium' and 'large' in terms of database size are operationally hard to define (especially in a sector-agnostic way) and also irrelevant to risk, arguably, if all other variables are kept constant.

Rule 2 (Note: copied from the Definition section above for easier review of the Rules)

While we understand the intention of the draft code is to capture biometric information as it relates to a biometric characteristic used for the purposes of biometric processing, we note the requirements under Rule 2 apply to "biometric sample" rather than "biometric information" (with the latter incorporating the concept of biometric processing). We assume this is not intentional, and is contrary to the intended scope of the draft code as set out in the Commissioner's guidance (see p. 6). In light of this, we recommend Rule 2 is amended so that it clearly applies *only to collection of a biometric sample "for the purposes of biometric processing"*.

Rule 3

Notice requirements

Rule 3 of the Code largely replicates the requirements of the existing IPP3, which provides that an agency collecting information directly from an individual must take reasonable steps to ensure the individual is aware of certain matters. However, Rule 3 goes further in that it requires the agency to take reasonable steps to ensure the individual is aware of certain additional matters over and above the matters provided for in IPP3.

Specifically, the requirements of Rule 3(1)(l) are potentially onerous for agencies and of little value to individuals. It may be quite onerous for agencies to make individuals aware of "any particular law that the agency is aware is likely to be relevant to the use or disclosure of the biometric information". It is not clear the nature of biometric information inherently requires individuals be made aware of all potentially relevant laws that may affect the use or disclosure of their information. The general policy of the Privacy Act is to accept that local and foreign laws may affect use or disclosure of personal information, and to address any unique risks posed by foreign laws through the cross-border disclosure requirements in IPP12, which is replicated in the Code through Rule 12. In light of this, we recommend removing Rule 3(1)(l) from the final version of the code.

Rule 3(1)(m) requires an agency to take reasonable steps to ensure an individual is aware of "the location of where the agency's assessment under rule 1(1)(c) or a summary of that assessment is available to view, if publicly available, or whether the assessment or summary is available on request". Consistent with our comment in relation to Rule 3(1)(l), this seems to be an onerous requirement on agencies with unclear benefits for individuals. There is a lack of distinction between informing or notifying people vs making people aware. Making individuals aware assumes that the agency confirms that the notification has been both perceived and understood is, for want of a better descriptor, 'a bridge too far'.

As Rule 3(1)(m) provides no clear material benefits for individuals, DINZ recommends removing this from the code.

Further feedback on guidance for Rule 3

The guidance suggests audio and verbal notices, but it is hard to prove and / or contest that a verbal notice took place or that the capture subject heard and understood the location / address of the accessible notice. A verbal notice that has enough built in checks to confirm that the capture subject heard and understood ("is aware of") each element of the notice will predictably increase service time and result in a negative customer experience.

Rule 6

Just a technical note here that might be useful in the guidance: for an agency to be able to conclusively state what kind of information they hold on an individual, they will have to first collect not just the relevant **biographic** data (name/s, former / other name/s, date of birth, place of birth, or any agency-relevant identifier) but also a **biometric** sample in the biometric modality the individual suspects the agency might hold. Missed client links, twins, and identity fraudsters exist in virtually all databases, so for best practice the agency would need to run a 1:N search on the presumed **biometric** modality as well.

Feedback on guidance for Rule 6

The guidance states that individuals "might want access to both biometric information and results (outputs) from the biometric process". DINZ is unsure how agencies can comply with this in a way that a) is helpful to the requestor, and b) doesn't breach the privacy of an/other individual/s. An agency can presumably either communicate the dates, match scores and some random internal identifiers of candidates that John Doe's **probe** hit, as well as all dates, match scores and probe identifiers that hit John Doe as a **candidate**, but this is completely meaningless and presumably useless to the requestor. Disclosing more identifying information (such as, DoB or names) of the other identities in these comparisons on the other hand would harm the privacy of these other identities. Twins, same-sex close-age siblings, lookalikes and identity fraudsters could in fact cajole the agency into breaches: "Oh you had someone apply who auto-matched me on face, and was very close to auto-matching me on biographics? Brilliant, now I know my brother or lookalike did submit an application with your agency".

On p. 91 in the guidance on Rule 6, the scenario about the FR system used for building access management probably needs a similar explanation / confirmation route as above. If a non-resident asks whether a system has any images of him it is not enough to communicate the theoretical truth ("John Doe is not enrolled and therefore we will have no images of you, John Doe."), but you need to also go into a bit more epistemic depth by actually running their face against the system to confirm that no false positives were tripped by this person. Especially in the context of larger biometric databases and more relaxed image standards this is a must.

On p. 91 the guidance also assumes that a business can disclose the template without harming intellectual property rights. Our suggestion would be to check with the vendor / solution provider if this is indeed the case.

Rule 10

Feedback on Question 29.

"Do you agree there should be limits on using biometrics to categorise people into certain sensitive groups? Are you aware of any high-risk or beneficial use cases?"

One beneficial use case is to categorise people into skin tone groups with the intention to set skin-tone-specific
- lighting, focus, and pre-processing algorithms at the cameras and sensors,
- templating mechanisms and
- matching thresholds

in order to address any (remaining) light reflection / absorption differential.

Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand

Arguably, 21(1)(h) of the Human Rights Act could block classifying / categorizing for intoxication levels, which is presumably against the intention behind Rule 10(6) about operational safety vs alertness levels, and 10(7) about preventing threat to health (were the intoxicated person to operate heavy machinery, for example).

Rule 10(7)(a) considers "accessibility", but the current definition of accessibility does not consider that even in the absence of a disability, accessibility is desirable: non-native speakers of a target language are not disabled but could benefit from an audio signal processing algorithm that sorts them into native(-like) vs non-native speaker categories to facilitate access to translators, interpreters, or more readable documents. Or people wearing different types of footwear might pose different tripping, slipping, and catching hazards (for example on an escalator or construction site).

Individuals, for whatever reason, might want to know where they place on various continua along the categories of personality, mood, emotion, etc., but Rule 10(5)(b) seems to prevent them from consenting to and contracting such services?

Rule 13

Biometric Templates

As stated above, the feature vs template distinction needs more work in the Code draft, and until this work is completed (hopefully by adopting the ISO standard definitions), it is hard to constructively comment on the intent of Rule 13, but the change did not improve the clarity of this rule. The distinction between a feature set and a template as per the ISO definitions is that a template is a feature set that is stored for reference. So technically an unstored feature set cannot be assigned to an individual to use and re-use, or to be shared between agencies. For multiple agencies to use a shared template for the same individual, firstly a *near-deterministic* modality is needed, like fingerprint, iris or retina, and then the two agencies would need to use some interoperable templating mechanism (if not the same vendor). In a *probabilistic* biometric modality, like face or voice, even the interoperable templates wouldn't ensure that the extracted feature set-based identifier is uniquely identifying. Unless the inert templates are used as verbatim text instead of an identifier (instead of typing ABC123 on login, John Doe's client number is now the 20Kb's worth of proprietary, encrypted keyboard-smash encoding his fingerprints "IHDRxÄÕsDATxì½‡[TWÛÿûûWÎ9ïû{Ÿ÷Éc'&½ƒôÞ{ï"'RDé½e†azï bIbIlØ{ lÎµö6#2"), we are uncertain how the technical solution outlined in Rule 13 can be operationalized, or what problem it would solve.

Referencing Rule 13 while the face is the source of biometric system recognition, the template derived by the algorithm is only valid for a solution using that specific version of the algorithm. There is no unique template that identifies across agencies and there can be other elements that are encrypted with a face template that again make the template unique for that image at that time. Also there is the probabilistic matching element which is provided for the decision process. There needs to be a clear focus on the overall process as having more impact on privacy issues.

Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand