Ben Keith
BARRISTER

20 December 2024

Michael Webster
Privacy Commissioner
PO Box 10 094
Wellington 6140

Dear Commissioner

***Draft Biometric Processing Privacy Code*: Consistency with human rights obligations**
File reference: P118-8

1. Thank you for your instruction to review the consistency of the *Draft Biometric Processing Privacy Code (**Draft Code**)* with human rights obligations under New Zealand law.

2. I have reviewed the *Draft Code* together with the accompanying draft guidance, a substantial volume of underlying policy and consultation documents and a range of comparative material. As I set out in detail below, I conclude that the *Draft Code* meets the range of human rights obligations that it raises.

Rights and interests in the collection and use of biometric data

3. The starting point in assessing the compliance of the *Draft Code* with human rights obligations is to understand the ways in which the collection and use of biometric data may impact upon those rights.

4. In short:

   4.1. The extent of data that is or can be collected in practice is increasingly broad and detailed.[1] That data collection – much of which occurs through conscious, unconscious or even mandated self-provision of data by individuals, whether

[1] See, for example, Omer Tene "Privacy: The new generations" (2011) 1 Int Data Priv L 15, 21, observing that biometric information collection is not new:

> "The concept of identifying people using unique biometric features is not new; fingerprints were used as far back as ancient Egypt and Babylon."

but then noting – even as at 2011 – the collection of, for example, facial recognition technology, gait and other behavioural analysis and "iris and retina scans, hand geometry, ear shape, ... voice, odor, scent, and sweat pore analysis".

about themselves or others[2] – can be broadly divided into two categories:[3]

(a) What can be termed "physical/physiological characteristics" – that is, concrete data such as facial images, fingerprints and DNA; and

(b) What can be termed "behavioural characteristics", ranging from walking patterns to remote sensing of individual cardiac rhythms to forms of verbal expression.

4.2. The use of that collected data has also expanded markedly. In addition to the longstanding use of biometric for authentication of identity – that is, confirming the identity of a given individual by one-to-one comparison to retained fingerprints or photographs – current and emerging technologically enabled uses of biometric data extend into several further broad and in part overlapping categories:[4]

(a) *Identification / "one to many comparison"*: compilation of biometric data to allow matching of an individual's data against an identifying database, for example allowing facial recognition in a crowd;

(b) *Categorisation*: automated extraction or approximation of physiological characteristics, such as sex or age, from biometric data;

(c) *Profiling*: use of biometric data to connect the individual concerned to other data held about that person; and

(d) *Statistical inference / correlation*: use of biometric data to infer or approximate characteristics of the individual concerned.

4.3. These further, and increasingly powerful and/or more readily available, uses are often controversial and/or problematic. For example:

---

2 See, for example, Adam Joinson and Carina B. Paine "Self-disclosure, Privacy and the Internet" in Adam Joinson, Katelyn Y. A. McKenna, Tom Postmes & Ulf-Dietrich Reips (eds) *Oxford Handbook of Internet Psychology* (2009), 237; Annemarie Sprokkereef and Paul de Hert "Biometrics, Privacy and Agency" in E. Mordini and D. Tzovaras (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer, 2012) 81, 97-98.

3 See, for example, Office of the Privacy Commissioner (New Zealand) *Protecting your privacy in the digital age – Insights report* (2023) 12:

> "people's faces, eyes, fingerprints, voices, signatures, keystroke patterns, or even odours or the way they walk"

and Marcello Ienca & Gianclaudio Malgieri "Mental data protection and the GDPR" (2022) 9 J L & Biosciences 1, 3:

> "speaking rates in conversation, tone of utterances, frequency of social interactions, ambient conversations, responses to cognitive tasks, 3D navigation tasks, sleep patterns, purchase preferences"

4 European Union Agency for Fundamental Rights *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (2019) 7-9; Nessa Lynch, Liz Campbell, Joe Purshouse, Marcin Betkier *Facial Recognition Technology in New Zealand*: *Towards a Legal and Ethical Framework* (Law Foundation, 2020), pp 7:3-7:4. Lee Conde and Dan Jerker B Svantesson "The five generations of facial recognition usage and the Australian privacy law" (2024) 14 Int Data Priv L 247, 249-254.

(a) Even for relatively straightforward use, such as authentication, the fact that biometric information is for the most part immutable – individuals cannot alter their fingerprints – raises the risk of persistent identify theft;[5] and

(b) The further categories of use can be unexpected, intrusive and/or otherwise harmful.[6] A survey by Conde and Svantesson published earlier this year notes uses and/or claimed uses of facial recognition technology to infer both:[7]

(i) Information such as age, gender or ethnicity – which may be less surprising but can also be error-prone and/or enable unlawful discrimination; and

(ii) Further, likely less foreseeable and potentially highly sensitive information or approximations as to, for example:

> "... occupation, attractiveness, humorous[ness], perfectionism, self-reliance, openness to change, warmth, reasoning, emotional stability, dominance, rule consciousness, liveliness, sensitivity, vigilance, abstractedness, privateness, apprehension, social boldness, sleep disorder ... sexual orientation, social relations, kinship, body mass index, mental health disorder, openness, conscientiousness, extraversion, agreeableness, neuroticism, depression ... and political orientation.

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

"(i) the (commercial or medical) *context* of the data processing;

(ii) the (diagnostic, observational, or targeting) *purposes* of the processing;

(iii) the *interests* in the data processing (public interests in diagnoses or data analyses; private interests in enhancing mental functioning or improving one's wellbeing; solely commercial interests in exploiting cognitive biases of consumers; etc.)"

---

5 See, for example, United Nations High Commissioner for Human Rights *The right to privacy in the digital age* UN Doc A/HRC/39/29 (2018), 14.

6 See, for example, Sprokkereef & Paul de Hert above n 2, noting challenges for individuals and for regulators arising from factors including (at 87-88):

"- Function creep (as a process by which data are used for different purposes than originally collected for);
- Increased tendency to keep data on file for possible future use (rather than discard data);
- Mounting pressure on individuals to disclose personal information and allow data linkage both by government agencies and by business organisations (the latter mainly through internet);
- Proliferation of types of hardware that hold large data sets (USB sticks, small gadgets and portable computers, data holding phones and so forth) that pose new security risks."

7 Above n 4, 251. See also, for inferred data generally, Damian Clifford, Megan Richardson and Normann Witzleb "Artificial intelligence and sensitive inferences: new challenges for data protection laws" in Mark Findlay, Jolyon Ford, Josephine Seah & Dilan Thampapillai (eds) *Regulatory Insights on Artificial Intelligence* (Elgar 2022) 19,

8 Above n 3, 8 (emphases in original) and, further, 11-15 & 17.

and also the capacity and/or vulnerability of any particular individuals concerned.

Law reform

5. The advent of increasingly powerful and accessible tools to collect and use biometric data has led to calls for review and reform of data privacy and related laws, most notably in the 2020 General Assembly resolution *The Right to Privacy in the Digital Age*, including in respect of private actors, and the particular need for adequate substantive and procedural legal safeguards.[9]

6. Such tools can, further, pose challenges for regulatory measures that can otherwise protect or reconcile rights. Notably:

   6.1. Reliance upon user consent and/or opting-out as a safeguard is often more difficult: to take the examples above, the extent of the use(s) of particular biometric information and any associated risks, particularly of data used in combination, may make truly informed consent difficult in practice;[10]

   6.2. Increased technological capacity can mean that what appears to be relatively mundane data can generate highly sensitive data, as for example in the inference of clinical data from facial images;[11] and

   6.3. Most broadly, there is a necessary challenge in seeking both to regulate current technological means in a clear and efficient way, without unduly impeding benign or justifiable practices, while also ensuring that future and potentially unforeseen means and/or practices are safely regulated.[12]

Assessment of *Draft Code*

Outline of Draft Code

7. As provided for under ss 32-38 PA, the *Draft Code* modifies and in parts prescribes how the Information Privacy Principles (**IPPs**) are to be met in respect of biometric information.[13]

---

9 General Assembly Resolution A/RES/75/176 (2020) "The right to privacy in the digital age", 4; [6] & [7](c), (f), (g), (p) and (q); United Nations High Commissioner, above n 5; and see also for example Lynch et al, above n 4, pp 7:5-7:12.

10 See, for example, Yuanyuan Feng, Yaxing Yao & Norman Sadeh "A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things" *CHI '21* (2021); Robert Sloan & Richard Warner "Beyond Notice and Choice: Privacy, Norms and Consent" (2014) 14 J High Technology L 370.

11 See, for example, Clifford et al above n 4, 42 and cf Ienca & Malgieri above n 3, 11.

12 See, for example, Els Kindt *Privacy and Data Protection of Biometric Applications: A Comparative Legal Analysis* (Springer, 2013), 752-758.

13 While statutory powers to issue codes of practice that modify provisions of a primary are relatively uncommon and require careful consideration and safeguards (see, for example, Legislative Design and Advisory Committee *Legislation Guidelines* (2021ed), 79), similar – albeit often narrower – powers exist in privacy/data protection regimes in other jurisdictions and the particular code power was endorsed, with minor amendments, by the Law Commission in its 2011 review report as affording the means for enhanced privacy protections: *Review of the Privacy Act 1993 : review of the law of privacy, stage 4* (NZLC R123, 2011), 164-173.

8. In broad terms, the *Draft Code* does not modify six of the thirteen IPPs (4, 5, 7-9 and 11), makes minor modifications to four (2, 6, 12 and 13) and makes substantive changes to:

   8.1. IPP 1, which concerns the lawful purpose and necessity of collection of such information and in respect of which the *Draft Code* prescribes:

      (a) Purpose-related effectiveness and the need to dismiss any reasonable alternative option;

      (b) A detailed proportionality standard, which includes the extent of any privacy risk; whether the benefits outweigh the privacy risk; and cultural impacts and effects upon Māori. The *Draft Code* also includes a carefully framed definition of privacy risk in cl 3(2) and a contextual definition of benefit, which distinguishes between benefits to the individual concerned; to the public; and/or to other private interests in r 1(4).

   8.2. IPP 3, in respect of which the *Draft Code* adds a minimum notice obligation and a transparency requirement; and

   8.3. IPP 10, in respect of which the *Draft Code* limits certain uses of biometric information and, in particular, prohibits its use to categorise people, for example in respect of prohibited grounds of discrimination under the Human Rights Act 1993; infer mental, emotional and similar information; and generate health information, other than in certain exceptional contexts

9. The *Draft Code* also contains certain exceptions: notably, health information – including genetic and neurological data – remains subject to the *Health Information Privacy Code*; most private non-commercial activity is exempted; and certain exceptions for national security under the PA remain applicable.

Process followed in preparing Draft Code

10. Prior to the preparation and release of the present *Draft Code*, the Commissioner had already undertaken a series of prior public and/or stakeholder engagement steps: a position paper on biometric regulation under the PA was released in October 2021; a consultation paper on regulation of biometrics was published in August 2022; the exploration of a code of practice was announced by the Commissioner in December 2022 ; a discussion document, which set out detailed code proposals, was published in July 2023; and consultation on an exposure draft released in April 2024.

11. The broad benefit of these steps is that, as noted in the published summaries of submissions, the proposed terms of the *Draft Code* and its underlying analytical work were subjected to scrutiny from a diverse range of perspectives. More concretely, the 2024 exposure draft consultation document generated a number of "use cases", which were provided as part of submissions from commercial entities that collect and/or use biometric information and which allow the concrete working through of possible *Draft Code* provisions.

12. The *Draft Code* is also subject to a review/sunset provision, under which it will be reviewed in three years.

Rights engaged by collection and use of biometric information and by regulation

13. The regulation of the use of data engages human rights obligations, as affirmed in New Zealand law and in international human rights obligations to which New Zealand is subject:

    13.1. Directly, both because:

        (a) Such regulation does or may constrain affirmed rights: most notably, the *Draft Code* regulates the collection and dissemination of information and so does engage the freedom of expression affirmed by s 14 of the New Zealand Bill of Rights Act and art 19 of the ICCPR;[14] and

        (b) Such regulation is, equally, required by the right to privacy affirmed in art 17 ICCPR and also reflected in the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, and reflected in s 3 of the Privacy Act 2020 (**PA**). In particular:

            (i) The right to the "protection of the law" against interference with privacy under art 17(2) is not limited to protection against governmental intrusion, but extends to non-state activity;[15] and

            (ii) State or state-sponsored collection may also and in parallel engage rights against unreasonable search and/or surveillance.[16]

    13.2. Indirectly, because:

        (a) The collection and use of identifying data – whether by state or non-state actors – has the potential to curtail or "chill" a broad range of rights that, to varying degrees, can or do depend upon expectations of privacy, such as – for example – political or religious observance, association and assembly;[17] and

        (b) Collection and use may also facilitate breaches of other rights, for example if biometric information permits or even inadvertently results in gender,

---

14 See, for example, William Schabas *International Covenant on Civil and Political Rights: Nowak's CCPR Commentary* (3ed: Engel, 2019) 557 (art 19(2) ICCPR right to seek, receive and impart information); Christopher Docksey "Four fundamental rights: finding the balance" (2016) 6 Int Data Priv L 195, 196; David Erdos "Special, Personal and Broad Expression: Exploring Freedom of Expression Norms under the General Data Protection Regulation" (2021) 40 Ybk Eur L 398; and Katja Kukielski "The First Amendment and Facial Recognition Technology" (2022) 55 Loyola of Los Angeles L Rev 231.

15 Schabas, above n 14, 461-462; Timo Istace "Protecting the mental realm: What does human rights law bring to the table" (2023) 41 Neth Q Hum Rts 214, 226-232.

16 See, for example, *R v Alsford* [2017] 1 NZLR 710; [2017] NZSC 42, [38]ff.

17 General Assembly above n 9 , 2-3; Docksey above n 14, 207-209; Els Kindt "Biometric data processing: Is the legislator keeping up or just keeping up appearances?" in Gloria González, Rosamunde Van Brakel & Paul De Hert *Research Handbook on Privacy and Data Protection Law* (Elgar, 2022).

ethnicity or other forms of prohibited discrimination or if used to subvert democratic or other rights.[18]

Assessment of rights-consistency

14. From these starting points and taking the four categories of rights, as set out above, in turn, it is possible to reach four fairly short conclusions:

    14.1. The only provision of the *Draft Code* that directly restricts rights is the restriction and, in some respects, prohibition of certain forms of biometric data processing other than under certain benign exceptions. That restriction does constrain the s 14/art 19 right to freedom of expression, but can be seen to do so on the basis that those forms of use and collection of biometric data – for example, the inference of emotional states – put at risk privacy and other rights to an unacceptable degree. As such, and in light of the broad basis for such regulation; the extensive process pursued by the Commissioner; and the well-evidenced and widespread concern over the potential for harm from these forms of processing, it is possible to conclude that the limitation is justifiable.

    14.2. In terms of the right to privacy, the *Draft Code* constitutes a refinement and, in parts, a strengthening of existing protections and obligations under the PA with the object, and evident effect, of better addressing the particular risks and benefits of biometric data and does so from a substantial evidence basis. As such:

        (a) It is clearly within the object of art 17 ICCPR and the wider calls to review and where necessary reform relevant safeguards;

        (b) In particular, the incorporation of proportionality and consideration of alternative means into Rule 1 affords broad flexibility to reflect the balance of interests in any particular use, subject to the specific limitations and exceptions under the *Draft Code*; and

        (c) Proportionality standards, although a well-known tool in human rights instruments,[19] have been criticised as unduly broad; at risk of unclear or insufficiently protective interpretation; and/or onerous.[20] However, the carefully framed definition of proportionality in the *Draft Code* addresses those concerns in two respects:[21]

            (i) The detailed components of that definition follow accepted human rights standards and address identified areas of risk;[22] and

---

18 See,respectively and for example, the useful survey in Andrea North-Samardzic "Biometric Technology and Ethics: Beyond Security Applications" (2020) 167 J Bus Ethics 433, 442-443 and Mario Viola de Azevedo Cunha and Shara Monteleone "Data protection, freedom of expression, competition and media pluralism: challenges in balancing and safeguarding rights in the age of Big Data" in Pier L. Parcu and Elda Brogi(eds) *Research Handbook on EU Media Law and Policy* (Elgar, 2021) 235, 240-241.

19 See, for example, *Attorney-General v Chisnall* [2024] NZSC 178, [98]

20 See, for example, above n 12.

21 Above at [8.1(b).

22 See, for example, above at [4.2] and [4.4].

(ii) More practically, the careful framing of that definition enables structured assessment of compliance by the potentially broad range of public and private entities that may engage in biometric data processing subject to the *Draft Code*.

14.3. The question of "chilling" of other affirmed rights, such as expression, religious observance or association, is expressly addressed by cl 3(2)(c) of the *Draft Code*, which includes such adverse consequence within the scope of relevant privacy risks. These, in turn, engage the other *Draft Code* provisions.

14.4. Similarly, the question of discrimination or other harm is addressed through the express limits in r 10(5), which prevents use of biometric information for categorisation of individuals on discriminatory grounds and inference of emotional or other data.

15. It follows that the *Draft Code* is consistent with relevant affirmed rights.

Yours sincerely

Ben Keith