IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY

I TE KŌTI MĀTUA O AOTEAROA
TE WHANGANUI-Ā-TARA ROHE **CIV-2021-485-553**

BETWEEN	**TE POU MATAKANA LTD, TRADING AS WHĀNAU ORA COMMISSIONING AGENCY**
	FIRST APPLICANT
BETWEEN	**WHĀNAU TAHI LTD**
	SECOND APPLICANT
AND	**ATTORNEY-GENERAL**
	RESPONDENT

SUBMISSIONS FOR THE PRIVACY COMMISSIONER AS INTERVENER

24 October 2021

Judicial officer assigned: Gwyn J
Next event date: Hearing, 26 October

John Edwards / Amy de Joux
Privacy Commissioner
Te Mana Mātāpono Matatapu
PO Box 10 094
Wellington 6143
(04) 494 7080
Amy.deJoux@privacy.org.nz

Ben Keith
Thorndon Chambers
PO Box 1530
Wellington 6140
(04) 460 0744
ben.keith@chambers.co.nz

MAY IT PLEASE THE COURT

1. These submissions address two aspects of this proceeding:

   1.1 The interpretation and application of the provision for disclosure in r 11(2)(d) of the Health Information Privacy Code 2020 (**Code**); and

   1.2 The wider context of how questions of use and protection of individuals' health information on grounds of their own, others' or public health may be resolved through the application of interconnected data privacy and health rights, including in light of obligations under the Treaty and of evolving principle and practice connected with the current pandemic.

2. In summary:

   2.1 The parties' submissions indicate apparent agreement that the respondent can, under r 11(2)(d) of the Code, lawfully share individuals' data with the applicant:[1] that is, it is not in issue both that:

      2.1.1 It is not desirable or practicable to seek those individuals' consent; and

      2.1.2 Disclosure is necessary and effectual to address the risk to the health and safety of those individuals, others and/or the wider public.[2]

   2.2 Where the parties differ, as understood, is:

      2.2.1 Whether there is, from whatever source, a corresponding obligation to exercise that lawful power to disclose that data; and

      2.2.2 Noting that the respondent has declined to disclose that data to the applicants for the time being, but has left open the possibility that it may come to a different view in time, as other steps are taken and evaluated and also as the respondent continues to consult with others:

---

1 See for further and fuller analysis of r 11(2)(d) the Commissioner's November 2020 public statement "Privacy, Covid-19 and the 'Serious Threat to Public Health' exception".

2 See respondent's submissions (**RS**) at [1.3](b) & [3.4](a) though see 19 October decision paper, annexure to Joanne Gibbs' second affidavit, at [44] (not yet necessary) and see below at [2.2.2]).

(a) Whether it is lawful, including whether it is reasonable, to take that staged approach, noting the applicants' position that disclosure of individual data is necessary now to address an immediate threat;[3] and/or

(b) Whether the reasons given by the respondent – for example, the need to treat health providers equitably; the lack of consensus and degree of controversy over individual data sharing; and concerns over bullying or other misuse – are relevant and proportionate reasons.

Utility of the Privacy Act and its wider context

3. The purpose of these submissions – noting the extent of agreement and focus of disagreement between the parties – is to set out how the operation of the Code, the Privacy Act 2020 and the wider principles that underpin and inform those instruments may assist in addressing, and to some degree simplifying, the question before the respondent as the decision-maker and now before the Court.

4. The detail of the the Code is discussed more fully below, along with its wider statutory context. Put short, however, the starting point from a data privacy and rights perspective is that reflected in United Nations and other official statements concerning data privacy and COVID-19 response. As was for example put by the United Nations Special Rapporteur on the right to privacy:[4]

> "[R]esponses that are shaped by and respect human rights result in better outcomes in beating the pandemic, ensuring health care for everyone and preserving human dignity.
>
> While the priority is to save lives, fighting COVID-19 and respecting human rights, including the right to privacy, are not incompatible. … [T]he trust of citizens that their privacy … is being taken into account builds confidence and willingness to proactively support State measures …"

5. Further and as noted by the Special Rapporteur and others, these are not new issues. Human rights and privacy law long recognised that public health risks may routinely warrant, for example, mandatory notification of contagious

---

3 Applicants' submissions (**AS**) [24], [30], [42] & [66].

4 *Report of the Special Rapporteur on the right to privacy*, A/75/147, 27 July 2020, 3 at [2]-[3]. See also Professor Cannataci's 2021 report AS/76/220, 23 July 2021, which – though largely focused on failures to respect privacy rights, such as sharing of COVID app tracking data for unrelated purposes – comments at [75] that:

> "Robust national-level data protection laws … assist contact tracing and vaccination registration initiatives to commence, with due regard to protecting citizens' data and communicating that necessity to the community.

disease and other measures, notwithstanding the special and sensitive character of most health information.[5] Further and more specifically, such use of vaccination-related information – for example in World Health Organization vaccine certificates for international travel, first introduced in 1959 – is of some standing.[6]

6. The broad result is that, when taken together with – as noted in the United Nations and other statements – the need to save lives and, more widely and as required by the International Covenant on Economic, Social and Cultural Rights, the highest attainable standard of health:[7]

   6.1 Both the careful protection and the careful use of personal health data are integral to the pursuit of that standard; and

   6.2 In keeping with those statements and, in particular, rights to privacy and to health, the actions and decisions of public bodies must be proportionate and, particularly, evidence-driven.[8]

7. From that perspective, the Commissioner makes four points concerning the present proceedings.

Established principles governing the careful use of individuals' health information, including in response to pandemics and other threats

8. The first is that the Privacy Act does not create enforceable rights in this respect and, further, does not itself give rise to an obligation of disclosure.[9] Instead, that question is an administrative discretion on the part of the respondent.

---

5 See above n 4, [11]-[18] and see also, and for example, the discussion of OECD and EU instruments and statements in M Kedzior "The right to data protection and the COVID-19 pandemic: the European approach" (2021) 21 Academy of European Law Forum 533, 538, including a Council of Europe joint statement that "data protection can in no manner be an obstacle to saving lives and that the applicable principles always allow for a balancing of the interests at stake."

6 See, for example, Nicol Turner Lee, Samantha Lai & Emily Skahill "Vaccine passports underscore the necessity of U.S. privacy legislation" *Brookings Institution Techtank*, June 2021, noting use of vaccination cards from the 1880s onwards.

7 See AS at [46] and see, for implementing legislation and among many other provisions, s 3(1) New Zealand Public Health and Disability Act 2000, setting out purposes that include "the best care or support for those in need of services" ((a)(iii)); reduction of health disparities for Māori (b); and facilitation of access to and dissemination of information "to deliver, appropriate, effective, and timely health services, public health services and programmes" ((d)).

8 See, for example, Kedzior above n 5, 538 and 539.

9 *R v Alsford* [2017] 1 NZLR 710, [2017] NZSC 42 [64] per Arnold J for the majority, Elias CJ dissenting but not to this point at [119]: "the [Information Privacy Principles] ... allow the police to seek personal information other than directly from the person involved and allow

9. This said, however, the Act, the Code and the principles that underpin them do inform the exercise of that discretion, both at the level of principle and in practical terms:

9.1 The preconditions for disclosure under r 11(2)(d) are, themselves, demanding, in line with the sensitive character of health information and the imperative for individuals' and public confidence both that data will in general be kept confidential and that, where data is used, that occurs only when and to the extent necessary and under continuing safeguards. The fact that those preconditions are accepted to be met, here, is potentially relevant to the wider question of whether an obligation arises and, if so, when.

9.2 Further, and in terms of that careful protection and use and wider public confidence:

9.2.1 As above, the context of the Act, Code and other instruments indicates that while the pandemic is an exceptional event, at least in recent times, the use of individuals' health data as a response to pandemics and similar risks to individuals and public health is not new.

9.2.2 Further, and more practically, it is important to recognise that the Act and the Code are not displaced by the exception in r 11(2)(d). The respondents, were they to receive the individual data sought, would remain subject to the stringent requirements of the Code and other regulatory obligations: that is, and for example, they would remain subject to obligations to treat that data in confidence, to use it only for the purpose permitted and to retain it securely and for no longer than required.

9.3 The same conclusion – noting the reference to wider rights and interests in the stated purpose of the Privacy Act in s 3 and also in the Commissioner's duties under s 21 – may also follow from Treaty obligations, in particular in respect of equity and active protection.

(but do not compel) an agency to release information".

10. The result is that the body of rights in issue here do have substantive content: within the Privacy Act itself, and as noted in *Dotcom*, the "open-textured" and flexible character of procedural elements – rather than, as noted by the respondent, "rigid rules"[10] – within the Act sits alongside the binding and substantive rights that that Act and, here, other standards confer.[11]

Evidence-driven approach to specific questions of disclosure and use

11. The second point for the Commissioner is that the framework of privacy and health rights, and the need to act consistently with both, requires an evidence-driven approach. The terms of r 11(2)(d) of the Code – that is, that disclosure must be necessary in order to prevent or lessen a serious risk to health – and that wider context require that decisions are consistent with the available evidence both as to whether:

    11.1 It is necessary to disclose and use individuals' information; and

    11.2 That disclosure and use presents a realistic prospect of preventing or lessening the risk.

12. The utility of that point in this proceeding is, it is suggested, that it may simplify the question before the parties and the Court. While both parties' positions are to some extent reflective of wider policy arguments and considerations, the question before the Ministry of Health as respondent and now before the Court can – consistently with r 11(2)(d) and the obligations to protect life and to promote health – be understood in narrower terms.[12]

13. The reconciliation of rights and interests envisaged by the standards set out above necessitates an evidence-based and essentially objective assessment of respective harms and benefits. While the Commissioner does not, and could not either appropriately or practically, put a view as to the contending evidential positions in the case, the question framed by these standards is, on that evidence:

---

10 RS [4.6].

11 *Dotcom v Attorney-General* [2020] NZCA 551, [68]-[74], addressing the individual's substantive and legally binding right of access under s11 of the Privacy Act 1993.

12 See by comparison the respondent's concern for the wider policy context and the risk of precedent setting: RS at [2.2], [2.4] and [3.4]-[3.6].

13.1 Whether disclosure and use of individuals' information, as sought by the respondent and taking account of any adverse consequences, presents a prospect of greater protection of life and health; or

13.2 Conversely, whether the adverse consequences of disclosure in substance outweigh any benefit.

14. The answer to that question will, necessarily, depend on the state of the evidence at the particular time, both in terms of what evidence is available and what that evidence shows concerning:

14.1 The risk to individuals', others' and public health;

14.2 The anticipated effectiveness of disclosure and use of the requested information;

14.3 The anticipated adverse consequences, in terms of the protection of life and health, or other material and relevant harms, of that same disclosure and use; and

14.4 Whether there are other options to address the risk that lessen the privacy intrusion and resulting harms that are nonetheless effective to address the risk, including in light of the urgency of that risk and so whether it is possible to await the outcome of lesser measures.[13]

---

[13] See, for example, above at n 4 (saving lives the priority) and as a workable example of good practice, albeit in terms of individual disclosures concerning current patients – and so not including the material factors, here, of the benefits and/or detriments of disclosure involving individuals not currently patients - the factors set out in United Kingdom General Medical Council guidance *Confidentiality - Disclosures for the protection of patients and others* (2018):

"When deciding whether the public interest in disclosing information outweighs the patient's and the public interest in keeping the information confidential, you must consider:

a. the potential harm or distress to the patient arising from the disclosure – for example, in terms of their future engagement with treatment and their overall health
b. the potential harm to trust in doctors generally – for example, if it is widely perceived that doctors will readily disclose information about patients without consent
c. the potential harm to others (whether to a specific person or people, or to the public more broadly) if the information is not disclosed
d. the potential benefits to an individual or to society arising from the release of the information
e. the nature of the information to be disclosed, and any views expressed by the patient
f. whether the harms can be avoided or benefits gained without breaching the patient's privacy or, if not, what is the minimum intrusion.

If you consider that failure to disclose the information would leave individuals or society

15. In particular, viewed from the perspective of evidence-driven assessments of necessity and effectiveness required by r 11(2)(d) and these wider standards, the question may become simpler. For example:

15.1 The respondent has cited the need to "[treat] organisations fairly and equitably" as:[14]

> "… a major driver for consulting on and establishing the decision-making framework for data sharing in this case. … [O]ther organisations would also be offered analogous data solutions and a protocol needed to be introduced …"

and:

15.1.1 These wider questions of overall policy and wider principle are, of course, critical; but

15.1.2 It is possible to address the particular questions of necessity, efficacy and urgency that arise in respect of the applicants' request in the narrower context afforded by r 11(2)(d) and the other privacy and health rights above.

15.2 Similarly, and noting the respondent's observation that the applicants' proposal has not been in terms of seeking a contractual arrangement for the particular use of the requested data,[15] it may be thought that – if such an arrangement is an effective way of securing both appropriately careful use of data and better health and safety outcomes – that could be an outcome consistent with the effective operation of r 11(2)(d) and the wider rights and interests outlined above..

Public reassurance through the robust and transparent use of established principles

16. The third point for the Commissioner follow from the established principles set out above. As has been noted from, for example, the work of the Special Rapporteur, the relevance of privacy and human rights principles is not only the concrete point that those rights can be and are reconciled as necessary to protect the lives and wellbeing of individuals and the wider public, but also that those

---

exposed to a risk so serious that it outweighs the patient's and the public interest in maintaining confidentiality, you should disclose relevant information promptly to an appropriate person or authority."

14 Respondent submissions at [4.18].

15 Above n 14, [4.24].

individuals and the wider public can be reassured that their rights are being upheld and protected.

17. The practical importance of that point is that, for example, it is self-evident in the context of the pandemic and of vaccination in particular that information as to whether given individuals are not vaccinated is, inherently sensitive. What is also important to convey, however, is that if – for instance – the respondent were to allow the applicants to access and use that particular data:

    17.1 That use would, as above, be subject to all of the protections of the Privacy Act and the Code;

    17.2 Any use of that data beyond that permitted and envisaged and any failure to protect or use data appropriately, would be contrary not only to the Privacy Act and the Code but also to wider obligations of health providers; [16] and

    17.3 In particular – noting concerns over bullying or other harms[17] – that use would itself have to respect the confidentiality of the individuals concerned.

Significance of wider context, in particular in respect of vaccination information

18. The Commissioner's last and narrowest point is that the issues concerning disclosure of vaccination status, as in issue here, do not arise in isolation. As has been announced publicly, government-provided proof of vaccination will be available and may be required for access to a range of public settings and services.[18]

19. The utility of that wider practical context is not to understate the complexity and potential controversy of vaccination mandates or of encouraging vaccine uptake. Rather, the point is that some of that complexity and controversy falls to be addressed in a much wider context than the particular decision in issue in this case.

---

16 See below for discussion of, the obligations set out in the Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996, and professional obligations.

17 See, for example, AS at [105].

18 See, for example, https://covid19.govt.nz/covid-19-vaccines/getting-proof-of-your-vaccination/, stating that digital certificates will be available from the end of November and "may be required" to be shown.

Relevant law

20. The broad starting point is that the Privacy Act; the Code adopted under that Act; and wider data privacy law is directed both to:

    20.1 Afford protections for individuals in respect of their own data; and

    20.2 Enable and safeguard the use and disclosure of that data, including – as here – when and how data may be, and may need to be, used and / or disclosed without the prior consent of the individual(s) concerned.

21. That is reflected by the stated purpose of the Act (at s 3):

> "… to promote and protect individual privacy by—
>
> (a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and
>
> (b) giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.

22. Section 21 of the Privacy Act, though on its terms directed to the Commissioner's discharge of functions under the Act,[19] gives some indication of the content of those respective rights, obligations and standards:

> "The Commissioner must, in performing any statutory function or duty, and in exercising any statutory power,—
>
> (a) have regard to the privacy interests of individuals alongside other human rights and interests, including—
>
> (i) the desirability of facilitating the free flow of information in society; and
>
> (ii) government and businesses being able to achieve their objectives efficiently; and
>
> (b) take account of international obligations accepted by New Zealand, including those concerning the international technology of communications; and
>
> (c) take account of cultural perspectives on privacy; and

---

19 The Commissioner notes the reference to consultation by the respondent: see the second affidavit of Joanne Gibbs at [4], common bundle at 920. As indicated at 920, n 2, that has been directed towards "framework" principles – that is, ensuring that the Ministry applies a robust framework that takes into account the Privacy Act generally and the Code to support its end decision on any requests. The Comissioner has not taken a view on the merits of the particular information request to the Ministry of Health.

(d) consider any developing general international guidelines relevant to the better protection of individual privacy …"

23. In turn, the Code is issued by the Privacy Commissioner under s 33 of the Privacy Act and, under the Act, has the effect of modifying and substituting the thirteen general Information Privacy Principles provided in s 22. Materially:

23.1 The Code applies to health information relating to identifiable individuals. It does not apply to anonymous or aggregated statistical information where individuals cannot be identified.

23.2 The Code has been developed through a broad consultative process[20] and follows earlier consultation and iterations under the Privacy Act 1993 (rpld). The reason for the distinct Code is to reflect the particular characteristics of the health sector and health information:

23.2.1 Most health information is collected in a situation of confidence and trust in the context of a health professional / patient relationship;

23.2.2 Health information is often, though not always, highly sensitive in nature; and

23.2.3 The collection, compilation and use of health information is ongoing and interrelated: data collected as part of one episode of care is often required by the health agency and other health providers in the future.

24. The scope of the Code is broad:

24.1 It encompasses, in addition to information about the health of any individual and any health services, that person's medical history; any disabilities that he or she has or has had; results of tests or examinations; and information incidental to the provision of any health or disability service; and

24.2 The Code applies to any person or entity that provides health or disability services and also and particularly to the range of agencies set out in cl 4(2).

---

[20] See, for submissions made on the 2020 iteration of the Code, https://www.privacy.org.nz/privacy-act-2020 /codes-of-practice/hipc2020/hipc-submissions/ .

The applicants, and the providers that they work with, and the Ministry of Health are subject to the Code.

25. The Code also reflects, and falls to be applied within, its wider context.

26. The first aspect of that context is that the Code in part reinforces and/or is reinforced by the statutory and professional obligations that apply to health agencies and professionals:

26.1 Health agencies and health professionals subject to the Code are subject to the obligations set out in the Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996;

26.2 Professional and ethical obligations, such as those promulgated by the Medical Council of New Zealand for medical practitioners and the Nursing Council of New Zealand for nurses; and

26.3 General obligations, including as to informed choice, consent and confidentiality, applicable in the context of patient-professional relationships and wider work.

27. The relevance of those wider obligations is in part reflected by the differences between the generally applicable provisions of the Information Privacy Principles under the Privacy Act and the requirements of the Code. Put short, the Code gives particular expression to the principles of informed choice and consent:

27.1 The Privacy Act makes general provision for the use of individuals' information without consent to address a threat to the individual or others in IPP 11(1)(f):

> "An agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds, …
>
> (f) that the disclosure of the information is necessary to prevent or lessen a serious threat to—
>
> (i) public health or public safety; or
>
> (ii) the life or health of the individual concerned or another individual; …"

27.2 The Code replicates that provision in r 11(2) but adds the prior requirement that the agency that holds the data must also:

> "… [believe] on reasonable grounds, that it is either not desirable or not practicable to obtain authorisation from the individual concerned …"

Specific requirements of the Code and r 11(2)[21]

28. IPP2 and Rule 2 both provide that where an agency collects personal information, the information must be collected from the individual concerned. One of the exceptions is where the individual authorises the collection of information from someone else (see IPP2(2)(c), and Rule 2(2)(a)). Again, the Code emphasises the importance of that authorisation being informed - unlike IPP2(2)(c), Rule 2(2)(a) requires the individual is made aware of the matters set out in Rule 3(1) - including the purpose of collection, the intended recipients, whether the supply is voluntary or mandatory, and the consequence (if any) if all or any part of the requested information is not provided.

29. Rule 11 places limits on the disclosure of health information. Generally, information can be shared where it was a purpose of collection, or where the disclosure is authorised by the individual concerned (see Rule 11(1)(b) and (c)). However, a number of exceptions are set out in Rule 11(2) which recognise that other interests may be engaged and may take precedence. Notably:

29.1 While previous iterations of r 11(2)(d) required an "imminent" threat, the Code as now in place does not;

29.2 Plainly, however, the evidenced urgency or otherwise of the threat will bear on the decision to disclose – in particular, whether it is possible to pursue alternatives that may be less intrusive but perhaps also less effective and/or to await better evidence, including for example by pursuing and reviewing those alternatives.[22]

30. These provisions enable, but do not in themselves require, the sharing of information where is either not practicable or desirable to get the individual's authorisation and one of the exceptions set out in Rule 11(2)(a) - (l) applies,

---

21 See also above n 1.

22 See, for example, *Henderson v Privacy Commissioner* (Unreported, High Court Wellington, CIV 2009-485-1037, 29 April 2010) [79]ff (imminence of threat justifying more intrusive disclosure).

Wider statutory and privacy/human rights context

31. The further context to the Privacy Act and the Code, in respect of health information, is that other legislation authorises, and in some instances requires, certain disclosure of particular health information. In addition to the human rights standards already noted:

    31.1 There are a number of statutes that require reporting of certain health conditions, or have information requirements relating to the supply of certain medications or treatments. By way of example, ss 74, 74AA and 74B of the Health Act 1956 requires health practitioners and testing laboratories to notify certain infectious diseases to a medical officer of health and, in some cases, a local authority too. That is the mechanism by which positive test results of COVID-19 must be reported to medical officers of health;

    31.2 Other statutes require reporting of certain matters so that an identified risk or event can be managed or inquired into by other organisations. For example, the Land Transport Act 1998 requires health practitioners to notify the Land Transport Agency if they think that the public safety requires that one of their patients should not be driving and that they are likely to do so;[23] and

    31.3 There are also statutes that allow disclosure, but only if a request has been received:

        31.3.1 Section 22C of the Health Act 1956 allows disclosure to specific people where it is required by them for specific purposes;

        31.3.2 Information may also be disclosed on request to a DHB employee, provided that it is essential for the purpose of exercising the Board's power, duties or function under the New Zealand Public Health and Disability Act 2000 s 22C(1)(a)(ii) and (b)(j); and

        31.3.3 Information can be obtained through the grant of production orders under the Search and Surveillance Act 2012 or requests by

---

23 Section 18 Land Transport Act 1998.

Police or Oranga Tamariki under section 66 of the Oranga Tamariki Act 1989.

31.4 Some statutes also create a positive duty to consider a request, and the framework that the agency must follow. For example changes were made to the Oranga Tamariki Act 1989 by the Children, Young Persons and Their Families (Oranga Tamariki) Legislation Act 2017, and information sharing provisions were included in the Family Violence Act 2018, to facilitate the sharing of information between relevant agencies, including health agencies, where there were safety concerns about the safety of children, or to stop and prevent family violence. These information sharing provisions which came into force in 2019 set out a number of principles to guide agency decision making. Both of these Acts put safety first: that is, when considering whether or not to disclose, both Acts make it clear that agencies must have regard to the principle that the well-being and best interests of the child or young person, or helping to ensure that a victim is protected from family violence, "should usually"[24] or "in general"[25] take precedence over any duty to keep the information confidential.

32. The broadest context to the Privacy Act and Code, and to the wider issues raised by this proceeding is – as reflected in the statement of purpose in s 3 – the body of international and comparative data privacy and wider human rights law already noted above.

B Keith / A de Joux
Counsel for the Commissioner as intervener

---

24 Section 21(2) Family Violence Act 2018.
25 Section 65A(2) Oranga Tamariki Act 1989.