IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY

I TE KŌTI MĀTUA O AOTEAROA
TE WHANGANUI-Ā-TARA ROHE **CIV-2021-485-624**

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

23 November 2021

Judicial officer assigned: Gwyn J
Next event date: Hearing, 25 November

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 are filed further to the Court's grant of leave to intervene and, as indicated, address:

    1.1 The further and more detailed questions now raised by the claim as to the application of the standards of necessity, efficacy and urgency under the Privacy Act 2020 (**Act**) and the Health Information Privacy Code (**Code**), which raise questions of the interpretation and application in practice of those provisions; and

    1.2 In addition, the claim and the terms of relief now sought by the applicants may also raise questions as to how the requirements of the Act and the Code may more broadly assist in resolving the claim.

2. The intervener's position, put short, is that:

    2.1 The Act and the Code provide not only a series of substantive legal standards for decisions to disclose individual data without consent, but also – in permitting that disclosure where necessary to address serious risk – constitute a legislative judgment that such disclosure is permissible. As reflected in the relevant rule and also in context, notably the report of the United Nations Special Rapporteur cited by the Court in the first proceeding:[1]

> "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 …"

    2.2 The result, as said in the first proceeding, is that decisions concerning disclosure ought not be complex. In this context, that is for at least three reasons.

        2.2.1 The legislature has already made the judgment that disclosure of individuals' data is justifiable where necessary to protect against serious risk. The Act, as reflected by s 3(a),[2] is concerned with both

---

1 *Report of the Special Rapporteur on the right to privacy*, A/75/147, 27 July 2020, 3 at [3], cited [2021] NZHC 2942 (***Te Pou Matakana v Attorney-General (No 1)***) [59].

2 "The purpose of this Act is 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,

protection and use: as sometimes said, it is a "how to", not a "don't do".

2.2.2 Further to that "how to" point, and as also noted in the Court's first judgment, disclosure of data remains subject to and is in substance conditional upon compliance with the other requirements of the Act and the Code. The result is that that compliance is an integral part of a decision to disclose, both because compliance must be assured and because compliance is the means to secure and maintain the trust to which the Special Rapporteur refers.

2.2.3 Last, the requirement under the Act and the Code for evidence- and rights-based decisions is not, and in particular in the context of urgency cannot be, a counsel of perfection.[3]

2.3 Following from these points, the question raised by the parties' different positions is, in very broad terms, that of response to urgency and, particularly:

2.3.1 The scope for evidence-gathering and, more widely, for reliance on alternative steps as a reason to reject the necessity of a request must take account of that urgent context.

2.3.2 In that urgent context, the imperative is not to seek a perfect solution but rather to determine whether a given disclosure is required to address the serious risk in an effective way.

2.3.3 Most practically, the scheme of the Act and the Code do provide a means to answer points of the kind apparently in dispute here. Where, for example, an identifiable population can be shown, by evidence, not to require the disclosure in order to address the serious

---

while recognising that other rights and interests may at times also need to be taken into account; ...".

[3] See, similarly, *Commissioner of Police v Director of Human Rights Proceedings* (2007) 8 HRNZ 364 concerning the related provision for use of information for other purposes where necessary for law enforcement purposes, now in s 22, Principle 11(1)(e) (at [54]):

"it should not be necessary, in order for an agency to bring itself within exception 11(e)(i), to show that without the disclosure some event would occur which would constitute a breach of law, ... In our view, that balancing is achieved by the agency's belief being subject to the objective criteria that it has to have been formed on reasonable grounds. ... The necessity might arise in many different ways ...."

risk, then the apt approach is to use data-matching or other measures to exclude that identifiable group.

2.3.4 More widely, and while noting the concerns for privacy raised by members of the public and cited in the respondent's second decision, the Act and the Code do provide the necessary answer. The premise of both, and of r 11(2)(d) in particular, is that disclosure is permissible to address serious risks, whether to the individual concerned or to the wider community. The point is not only that, as above, that judgment has already been made but also that, as in the excerpt from the Special Rapporteur, saving lives is the imperative.

Further questions arising in this second proceeding

Interpretation of the Act and the Code in Te Pou Matakana v Attorney-General (No 1)

3. The starting point for these submissions are the findings of this Court concerning the Act and the Code in its 1 November judgment in the first proceeding between the parties.[4] First, as to the :

3.1 The framework under the Act is directed to protect an individual's right to privacy in their own personal information, while recognising that other rights and interests may at times need to be taken into account ([31], citing s 3(a)). The Code, for its part, reflects the particular characteristics of health information (at [33]):

3.1.1 Most health information is collected in the context of confidence;

3.1.2 It is often highly sensitive; and

3.1.3 The collection, compilation and use of such information is ongoing and interrelated: data collected by one agency on a given occasion is often required by that agency or others in future.

3.2 The Act and the Code provide for the disclosure and use of information without individuals' consent where and to the extent that that is necessary to address serious risks to health, but that disclosed information itself

4 Above n 1.

remains subject to the protections and restrictions under both ([36] and [38]).

3.3 The wider context to the Act and Code are the human rights both to privacy and to health, which are – quoting the United Nations Special Rapporteur on the right to Privacy – "not incompatible", that is, that robust privacy protections promote public confidence and, more widely, (at [59]):[5]

> "… responses 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."

3.4 In consequence, actions and decisions of public bodies as to, in terms of r 11(2):

3.4.1 Whether it is necessary to disclose and use individuals' information; and

3.4.2 Whether that disclosure presents a realistic prospect of preventing or lessening the health risk:

must be proportionate and evidence-based (at [61]).

3.5 In practice, that requires an objective and evidence-based assessment of (at [63](a)-(c)):

3.5.1 The anticipated effectiveness of disclosure and use of the particular information;

3.5.2 The anticipated adverse consequences of that disclosure; and

3.5.3 Whether there are other, less intrusive and/or adverse option that are nonetheless effective, such that it is possible to await the outcome of those lesser measures.[6]

Further and more particular questions arising in this proceeding

4. This further proceeding takes issue with the second decision of the Director-General of Health of 5 November, made consequent on orders of this Court. It is

---

5 Above n 1.

6 See also [72] ("'least-privacy invasive' test relevant if two equally effective measures").

in particular, in terms of the relevance of the Act, Code and the principles given above, pleaded that the second decision:

4.1 Addressed the relative efficacy of the disclosure – that is, what could be done without the data, not whether more could be done with it (SOC [69.1]) and/or reliance on a "less privacy intrusive alternative" without assessing whether that alternative was equally effective (SOC [71.1];

4.2 Failed to address urgency – that is, the identified need to reach all of the eligible population as soon as possible (SOC [69.2]/[71.2]);

4.3 Failed to address the option of differentiating in its response between the disclosure data for areas in which disclosure was considered warranted and areas where not warranted (SOC [69.4]); and

4.4 Relied upon an irrelevant consideration – that, is whether Whānau Tahi is subject to iwi oversight and/or iwi support or opposition, without further assessment – in assessing necessity, efficacy and adverse consequences (SOC [71.3]/[77.2]).

5. In addition to the particular and underlying factual matters in issue in respect of the pleaded claims, these pleadings do raise and/or further clarify important questions concerning the Act and the Code. Addressing each briefly in turn:

5.1 The question of whether disclosure and use of data presents a realistic prospect of preventing or lessening the risk to health is not a relative assessment. The premise of r 11(2)(d) is that disclosure is permitted where there is a serious risk; where disclosure presents a realistic prospect of addressing that risk; and where there is not an equally effective alternative to disclosure. In terms of those three requirements:

5.1.1 If there is another means that does not involve disclosure but does address the risk, then necessity is not made out and r 11(2)(d) is not engaged; but

5.1.2 If there are other means that do not involve disclosure but is not effective to address the serious risk, whether wholly or partly, then necessity is made out; but

5.1.3 It may be relevant to the assessment of adverse consequences and their weighing in assessing the proportionality of disclosure – depending upon the particular facts – if:

(a) The other means was shown to be substantially effective in addressing the risk, while the means that requires disclosure, though more effective, was shown to cause adverse consequences disproportionate to that difference in efficacy; and/or

(b) The adverse consequences of disclosure were shown to be such that while disclosure might, for example in the present case, reach people at risk who would not otherwise be reached, that disclosure might also deter people at risk who could be reached by those other means.

5.2 On the second point as to urgency, the intervener's position – as put in the first proceeding – is that:

5.2.1 Rule 11(2)(d), unlike the position under the Privacy Act 1993 prior to the 2013 Amendment Act[7], is not limited to urgent threats. However, where urgency is present, s 7(1) provides that timing of the threat is a factor in assessing whether a serious threat is present and time is relevant both to necessity and efficacy: for example, a less privacy intrusive alternative that is effective in some respect but does not meet the urgency of the risk is not an effective alternative for the purpose of the rule; and

5.2.2 More widely, where the r 11(2)(d) requirements are met, the rule permits disclosure but does not – of itself – require it. However, the requirements of necessity and efficacy are stringent and, if met and may demonstrate that other obligations – for example, the right to

---

7 Section 5. See for legislative history the Privacy (Information Sharing) Bill 2011, explanatory note at p 2:

"Currently , that threat must also be imminent for the information to be shared. This could prevent agencies from sharing information, where a failure to share could have serious consequences, merely because those consequences are not imminent. Instead, agencies will be required to consider the time at which the threat will occur , as well as the likelihood and severity of the consequences, in deciding whether the threat is serious."

the highest attainable standard of health – do require that disclosure to occur.

5.3 On the third point as to partial or differentiated disclosure – that is, disclosing such data for which necessity and efficacy is made out but not otherwise, the requirements of necessity and efficacy are not, or at least not inherently, polar. As reflected by the requirements of the rule, as described above:

5.3.1 An agency considering disclosure under r 11(2)(d) can only disclose such data as meets those two requirements; but

5.3.2 Unless, on the particular facts, disclosure is an all-or-nothing exercise – for instance, if the data in issue were for some exceptional reason unable to be sorted, matched or otherwise made to correspond to the scope of necessity and efficacy:

(a) The premise of r 11(2)(d) is that the disclosing agency must in fact undertake that exercise if it is proposing to disclose;

(b) It does not appear consistent with r 11(2)(d) or its wider human rights context to decline to disclose notwithstanding necessity and efficacy are made out because of overbreadth. Plainly – and bearing in mind the availability of sophisticated and privacy-protective sorting, matching and other techniques – that overbreadth may be addressed; and

(c) If that is not possible, however – either because the data to be disclosed is not held in a way that allows such differentiation or because matching data is not available – r 11(2)(d) nonetheless permits disclosure of undifferentiated data if that is a proportionate response to the serious risk. Proportionality requires, in turn, an assessment of whether, bearing in mind attendant protections, that broader disclosure gives rise to harm sufficient to displace the serious risk.

5.4 The fourth issue of iwi oversight and/or opposition raises again the point made in the intervener's submissions in the first case that r 11(2)(d) does to some degree simplify the question for the disclosing agency:

5.4.1 Plainly, it may well be material to the necessity or efficacy of disclosure and/or to the extent of adverse effects if the evidence is that iwi are opposed, for example, because:

(a) Disclosure of data of individuals affiliated to a given iwi is unnecessary because that iwi has itself taken effective steps to protect those individuals; or

(b) Disclosure of individuals' data will be ineffectual or counter-productive in practice unless those individuals' iwi consent or are otherwise involved.

5.4.2 However, and to return to two general aspects of r 11(2)(d), iwi concerns for particular affiliated individuals may be answered through steps such as:

(a) Data sorting or matching, as above; and/or

(b) More broadly, transparent management and protection of data in a way that allows iwi to ensure that data is disclosed, used and retained – or deleted – in a way that upholds the rangatiratanga of that iwi and the confidence of those affiliated to it.

Means under the Act to resolve any potential impasse

6. The further and broader point for the Commissioner concerns relief: perhaps understandably, given the accepted urgency of the circumstances and that this is the second decision and second proceeding concerning this data, the applicants have sought particular and mandatory relief in the form of orders for particular disclosure.

7. As said by the Special Rapporteur and quoted in the first judgment, public confidence in the robustness of privacy protections is integral to effective health responses to the pandemic. However, it is said in the decision paper in issue in this proceeding that (at [38]):

> "[The Director-General's advisers] would not recommend placing great weight on the notion that protections provided by privacy law induce any comfort among relevant populations. We see little evidence to support that. Indeed, the number and tone of the complaints received by the Ministry … suggest the prospect of sharing individual Māori health information with the applicants has

given rise to considerable anxiety for some."

8. That observation – and, particularly, that anxiety – is a matter that should and, it is hoped, can be addressed. The possible means of doing that include:

8.1 As above, taking steps to refine and control the extent of disclosure so that it is shown to be both no more than necessary and safe; and

8.2 Transparency in the management and protection of data, including for example through:

8.2.1 Publicity concerning systemic safeguards – that is, and in keeping with the Special Rapporteur's observations above, promoting public understanding of any disclosure and attendant protections as a means of lessening adverse reactions; and

8.2.2 Specific and concrete safeguards such as scope for individuals to opt out or, as already proposed here, recording of refusals by contacted individuals; and

8.2.3 Visibility of relevant systemic safeguards for iwi or others.

B Keith / A de Joux
Counsel for the intervener