IN THE SUPREME COURT OF NEW ZEALAND **SC 51/2023**

I TE KŌTI MANA NUI Ō AOTEAROA

BETWEEN	**MAHIA TAMIEFUNA**
	Appellant
AND	**THE KING**
	Respondent

SUBMISSIONS FOR THE PRIVACY COMMISSIONER | TE MANA MĀTĀPONO MATATAPU AS INTERVENER

1 March 2023

Counsel certify that, to the best of their knowledge, these submissions are suitable for publication and does not contain any information that is suppressed.

Joanna Hayward / Amy de Joux
Office of the Privacy Commissioner
Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
(04) 474 7590
legal@privacy.org.nz

Ben Keith
Woodward St Chambers
PO Box 655, Wellington 6140
(04) 473 3133 / 021 678 739
contact@benkeith.co.nz

Received Supreme Court 1 March 2024 electronic filing

MAY IT PLEASE THE COURT

1. The present appeal, and the points put both for Mr Tamiefuna and, in supporting the decision of the Court below on other grounds, for the Crown raise basic but far-reaching questions over how the collection, retention and use of information by the state is to be governed.

2. In short, the Commissioner submits that:

   2.1 The right against unreasonable search and seizure in s 21 of the New Zealand Bill of Rights Act (**Bill of Rights Act**) falls to be interpreted consistently with the right to privacy. That right, and the obligation of consistent interpretation, stems from:

      2.1.1 The longstanding common law right against state intrusion absent prescriptive judicial warrant or prescriptive statutory power; [1]

      2.1.2 The affirmation and development of that right under art 17 of the International Covenant and Civil and Political Rights (**ICCPR**), in particular in respect of technologically assisted information-gathering, analysis and dissemination;[2] and

      2.1.3 The implementation of that right through not only s 21, but also:

         (a) The information privacy principles (**IPPs**) in s 6 of the Privacy Act 1993, as in force at the time of the vehicle

---

1 See, particularly, *Entick v Carrington* (1765) 19 State Tr 1030 , 95 ER 807:

> "Has a Secretary of State a right to see all a man's private letters of correspondence, family concerns, trade and business? This would be monstrous indeed ..."

and for discussion in respect of privacy law see, for example, *Hosking v Runting* [2005] 1 NZLR 224, [2] per Gault P (*Entick* as remedy for interference with rights); C Forcese "The Limits of Reasonableness: The Failures of the Conventional Search and Seizure Paradigm in Information - Rich Environments" *Privacy Commissioner of Canada: Insights on Privacy* (2011); H Winkelmann "Sir Bruce Slane Memorial Lecture" (November 2018).

2 NZTS 1978, No 19 and see, for example, *Minister of Justice v Kim* [2021] 1 NZLR 338, [2021] NZSC 57, [282] (interpretation consistent with international obligations).

stop in November 2019, and since reenacted as s 22 of the Privacy Act 2020 (**Privacy Acts**);[3] and

(b) The detailed provision of warrantless powers of surveillance, search and seizure and of the conditions upon and limitations to those powers and the retention and use of information thereby obtained.

2.2 That right to privacy bears upon each of the questions in issue: the scope and content of s 21; the intersection of s 21 with prescribed statutory powers and with "third source" powers; and the remedy for unlawful search, as in issue under s 30 of the Evidence Act 2006 (**EA**):

2.2.1 First, as to the scope of the s 21 right against unreasonable search and seizure, the right to privacy entails consideration of the overall context and effect of the state action: in the instant case, that means that the question of whether the action of the Police officer in photographing of the appellant was a search and/or seizure must take account of:

(a) The conduct of that action in the context of – and, here, consequent on – the exercise of mandatory powers; and

(b) The retention, dissemination and analysis of the photograph and related information through the Police NIA database.

2.2.2 Second, as to the intersection of the s 21 right with prescribed statutory powers and with "third source" powers, the s 21 right itself and the wider right to privacy requires that state intrusions into privacy are prescribed by law: that is, not only authorised by law but sufficiently prescriptive that its terms are known and effectively enforced. The consequence is that:

---

3 The material provisions of the 2020 Act entered into force on 1 December 2020: see s 2(2). The provisions of the two Acts material to the present case do not markedly differ but are cross-referenced below.

(a) Where relevant statutory powers, and limitations upon those powers, have been prescribed – here, certain information-gathering powers under the Land Transport Act 1998 (**LTA**) and powers in respect of particulars and photography under the Policing Act 2008 (**Policing Act**) – the starting point is the presumption that those powers are exhaustive; and

(b) If a "third source" power is nonetheless found, its terms and limitations must be similarly prescribed and enforceable.

2.2.3 Third, the corollary of the right to privacy is that a breach of that right by the state must have an effective remedy, such that s 30 of the Evidence Act may be read to permit admission of unlawfully obtained evidence only in exigent circumstances.

2.3 The broader point for the Commissioner is that, in addition to the requirement of interpretation consistent with common law rights and international obligations, the further utility of the privacy right – derived, as above, from common law principle; the New Zealand statutory scheme, including but not limited to the 1993 and 2020 Privacy Acts and the IPPs; and art 17 and its counterparts – is that it affords a prescribed and legitimate basis on which to interpret and apply both s 21 and s 30. What that means is that, in particular:

2.3.1 The advent of ever more powerful and efficient tools to gather, analyse and disseminate information – whether the fairly straightforward, though powerful, tools used here or other measures – makes the application of s 21 and cognate rights more complex, but no less protective. As put by the United States Supreme Court in *Jones*, the right against unreasonable search and seizure must be construed in the face of such tools so as to maintain the same protection against state intrusion.[4]

---

4 *United States v Jones* 565 US 400 (2012), slip opinion at 5-10 (concerning GPS vehicle tracking and declining to hold that no privacy interest in vehicle movements):

2.3.2 The protection afforded by the requirement that an intrusive power be prescribed by law is practical and far-reaching. As observed by the European Court of Human Rights, such law:[5]

> "… must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise …
>
> it is … essential … to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."

and, further and as underpins both the s 21 right and the right to privacy, that concept of arbitrariness is not – in the context of state information-gathering – limited to capricious measures, but rather reflects and protects the rule of law. That is, ss 21 and 30 ought not be viewed as a conflict between a state or public interest in securing as much information as possible and the necessary protections for individual privacy, but rather the fundamental interest in ensuring that rights are upheld under law.

How information privacy principles relevant to s 21 / s 30 assessments

Information privacy principles in the court below

3. The Court below found that breaches of the information privacy principles provided in the Privacy Acts were material to the assessment under s 21. Notwithstanding that the Acts provide that the principles do not confer enforceable individual rights:[6]

"At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"

and see also and particularly the concurring observations of Sotomayor J slip opinion at 2-3; 16-17, later endorsed in *Carpenter*, below n 28, that the expectation of privacy test ought take into account the particular power of GPS monitoring; the potential to "store such records and efficiently mine them for information years into the future"; and the evasion of ordinary checks – "limited police resources and community hostility" - as well as the prospect of unfettered executive discretion outside judicial or legislative oversight.

5 *Marper v United Kingdom* [2008] ECHR 1581 (GC), (2009) 48 EHRR 50, [95] & [99].

6 Judgment under appeal at [83] & [80]-[82], **Case 36**.

> "While it is clear from s 11(2)[7] of the Privacy Act that (with an exception not relevant here) breaches of any of the information privacy principles do not create rights enforceable in a court of law, we think the principles must be relevant to the judgment of a court considering what reasonable expectations of privacy ought to encompass in accordance with modern societal expectations."

4. In the instant case, the Court found that the photographing of the appellant by Police had breached three of the principles:[8]

   4.1 First, principle 1(a) requires that an agency may only collect personal information as is necessary for a lawful purpose. Here, because the Land Transport Act 1998 does not authorise the taking of photographs for other purposes and, further, the photographs were taken for "intelligence" purposes and not for a then current investigation, they did not meet that requirement;

   4.2 Second, principle 3(1) requires that the collecting agency takes reasonable steps to ensure that the person concerned is aware of – among other matters – the collection, its purpose and its statutory or other legal basis, if any. That did not occur and the underlying purpose – that those providing information voluntarily do so on an informed basis – was not met;[9] and

   4.3 Third, principle 9 requires that information, once collected, must be held for no longer than is required for the purposes for which it may lawfully be used. As the photographs were not taken for the purpose of an investigation, they should not have been retained. The Court commented:

   > "[Principle 9] stands against the casual taking and retention of photographs on the basis that, some day, they might be useful."

   and contrasted the prescriptive statutory scheme for the collection, retention and destruction of photographs and other particulars in ss 34-34A of the Policing Act 2008.

---

7 Now reenacted as s 31(1) PA2020. The exception concerns the right of access to information held by a public sector agency in principle 6(1).

8 See, for the principles, PA1993, s 6 and – as enacted without amendment – PA2020, s 22.

9 The Court also observed (at [81]) that it had not been suggested that the exception to principle 3 for necessary law enforcement purposes, as addressed below at n 25, was made out.

5. The Court below in turn found the photography to be both unlawful as unauthorised and unreasonable under s 21.[10] It did not, however, further address the principles in its application of s 30.

Information privacy principles in Alsford

6. This Court previously considered the information privacy principles in relation to s 30 in its decision in *Alsford*, the majority accepting the relevance of the principles but expressing doubt over their significance:[11]

> "Accordingly, while we accept the possibility that the fact that personal information was obtained in breach of the privacy principles will be relevant under s 30, we think it unlikely that it will be of any independent significance in many instances. This is because what will be significant to the s 30 assessment is the nature of the conduct at issue rather than the fact that it constitutes a breach of the privacy principles."

the majority decision noting in particular that:

6.1 Section 11(2) of the 1993 Act, reenacted as s 31(1), provides that the principles "do not confer on any person any right that is enforceable in a court of law": instead, as the Court observed "the Act contains its own enforcement mechanisms";[12]

6.2 This said, the principles may bear on the interpretation of – in that case – the Search and Surveillance Act 2012 (**SSA**), given that Act's cross-reference to the Privacy Act;[13] and

6.3 The broad definition of personal information and the potential for breach to "cover the spectrum from minor to significant".[14]

---

10 Judgment under appeal [97], **Case 41**.

11 *R v Alsford* [2017] 1 NZLR 710, [2017] NZSC 42,, [40].

12 Above n 11, [37].

13 Above n 11, [38], citing the purpose provision in 5 SSA. Section 5 provides in relevant part:

> "The purpose of this Act is to facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values by—
>
> (b) providing rules that recognise the importance of the rights and entitlements affirmed in other enactments, including the New Zealand Bill of Rights Act 1990, the Privacy Act 2020, and the Evidence Act 2006: …"

The term "rules" refers to the powers and conditions given in the SSA: see, for example, part 2, subpart 1 "Rules about search warrants …" and s 125 (rules for searches of persons).

14 Above n 11, [39].

7. The Court also, though more briefly, addressed the relationship between the principles and s 21, declining to hold that compliance with the principles meant "there will be no search"; that the question of whether a search has occurred will depend upon whether there is a reasonable expectation of privacy in the particular personal information; and that the question will then be that of reasonableness under s 21.[15]

8. The Rt Hon Chief Justice, in dissent, disagreed with the reliance upon s 11 and more broadly did not adopt what Her Honour characterised as the majority position that "impropriety in the obtaining of evidence cannot be established by breach of the privacy principles but must be addressed under s 21 of the New Zealand Bill of Rights Act". Materially for present purposes, Her Honour observed that the scope of protection under the 1993 Act was relevant to the reasonable expectation of privacy. [16]

Reconciling the two approaches

9. The decision of the Court below and that of this Court in *Alsford* are, on their specific facts and as will be apparent, directed to different questions:[17]

    9.1 *Alsford* was, as has been set out, concerned with whether breach of information privacy principles rendered the warrantless access to subscriber information unlawful in terms of s 30; and

    9.2 The Court below, as in the excerpt above,[18] engaged with the principles in order to determine whether the photographs breached a reasonable expectation of privacy under s 21:

    and the factual contexts of the two decisions – the informative but less intrusive third party records in *Alsford* and the direct collection of identifying material following a statutory traffic stop and seizure here – are also plainly different.

---

15 Above n 11, [64].

16 Above n 11, [121], [123] and [194].

17 The respondent submissions cite (at [82]-[83]) passages from *Alsford* as concerning the relevance of the principles to "whether s 21 had been breached" but, as above, those are concerned with s 30.

18 Above n 6.

10. This said, however, and as put for the respondent,[19] the overall terms of the decisions do appear to represent two different conceptions of the relationship between the information privacy principles and ss 21 and 30:

    10.1 The doubt that the principles would be unlikely to be significant in many cases expressed in the majority decision in *Alsford* can be contrasted with the reliance – albeit as one factor – upon those principles by the Court below; and

    10.2 More narrowly, the approaches to the non-enforceability provision in s 11(2), now s 31(1), of the Privacy Acts differ: in particular, this Court in *Alsford* pointed to the distinct enforcement mechanisms under the 1993 Act and those mechanisms, though now strengthened, remain.

11. From that starting point, it may be that good or even compelling reason is needed to revisit the analysis given in *Alsford* or, at least, that the scope of *Alsford* requires clarification.[20] In either case, there are now several strong reasons to adopt the wider approach to the principles and s 21 taken by the Court below and, in particular, to revisit ss 11(2)/31(1).

Interpretation of s 21 as a right to privacy against state intrusion

12. The first, and simplest, reason is that s 21 is directed to, and must be interpreted and applied consistently with, the right to privacy as required by art 17 ICCPR and reflected by the principles. In line with the principles and as authoritatively stated in *Marper* in respect of the parallel privacy right in art 8 of the European Convention, the right to privacy requires that:[21]

---

19 See, particularly, [82], citation omitted:

> "When considering whether s 21 has been breached, the focus is the nature of the conduct rather than compliance with various privacy principles. Requiring trial courts to analyse those principles would add length, rather than depth, to the s 21 analysis."

20 See *Couch v Attorney-General* [2010] NZSC 27, [2010] 3 NZLR 149, [104] per Tipping J:

> "It would not be appropriate for this Court to regard itself as absolutely bound by its own previous decisions. No other comparable court now takes that approach to its own decisions. It is, however, highly desirable for the stability of the law, and the ability of citizens to order their affairs with confidence, that previous decisions of a final appellate court be departed from only in compelling circumstance."

21 Above n 5, [103].

12.1 The collection, use and retention of personal information is no more than is necessary and proportionate for a legitimate purpose;

12.2 State actions must be subject to safeguards at the point of collection, retention and destruction, and use.

13. The premise that rights against unreasonable search and seizure are to be construed as rights to privacy is of long standing. As put by Justice La Forest J, writing in the early and leading decision of the Supreme Court of Canada on the equivalent right in s 8 of the Charter in *Dyment*:[22]

> "Though rationalized in terms of property in the great case of *Entick v. Carrington* (1765), 19 St. Tr. 1029, 2 Wils. K.B. 275, 95 E.R. 807, the effect of the common law right against unreasonable searches and seizures was the protection of individual privacy. …
>
> The foregoing approach is altogether fitting for a constitutional document enshrined at the time when … society has come to realize that privacy is at the heart of liberty in a modern state. … The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state. "

and similar, and again long-standing, statements can be found in Fourth Amendment judgments of the United States Supreme Court.[23]

Relevance and utility of the principles

14. From that starting point, the right to privacy affords a robust and contextually informed standard for s 21: [24]

> "… in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained"

and the principles, as express, legislated and contextually flexible standards, allow that standard to be applied in a robust and transparent manner.

---

22 *R v Dyment*, [1988] 2 SCR 417, 426 at [16]-[17], citations omitted.

23 See, for example, *United States v Lefkowitz* 285 US 452, 464 (1932):

"The Fourth Amendment... is construed liberally to safeguard the right of privacy."

and *Wolf v Colorado* 338 US 25, 27 (1949):

"The security of one's privacy against arbitrary intrusion by the police … is at the core of the Fourth Amendment-is basic to a free society."

24 *Marper* above n 5, [67].

15. That can, in particular, be seen in the specific exceptions provided in several of the principles for law enforcement: to take the principles above, both the requirement of collection from the person concerned and the requirement to ensure awareness of the collection and its purpose are each disapplied if, in the particular circumstances:[25]

> "… the agency believes, on reasonable grounds, – …
>
> (b) that non-compliance is necessary—
>
> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
>
> (ii) for the enforcement of a law that imposes a pecuniary penalty; or …
>
> (c)/(e) that compliance would prejudice the purposes of the collection; …"

16. The application of the principles, including the standard of necessity on reasonable grounds under these exceptions, serves three purposes:

16.1 Most simply – and in particular in respect of state information-gathering that may not be or purports not to be subject to particular statutory schemes, as here and also in the practices canvassed in the joint report[26] – the principles provide both a substantive and a procedural check: it is necessary for the Police or others both to consider, and to be satisfied, that the exceptions are made out.

16.2 Further, the principles meet the requirement of the right to privacy that intrusions to privacy are not only authorised by some positive law but are prescribed by law, as for example in *Marper*:[27]

> "… the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of [the right to privacy in] Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision

---

25 Principle 2(2)(b) & (e); principle 3(4)(b) & (c).

26 *Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public* (September 2022).

27 Above n 5, [95] and see also Human Rights Committee *General Comment No. 16: Article 17 (Right to Privacy)* UN Doc HRI/GEN/1/Rev.1 at 21, [3]:

> "The term 'unlawful' means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of the law, which itself must comply with the provisions, aims and objectives of the Covenant."

> to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise."

16.3 Last, the principles are an express and legislated statement of the components of the right to privacy and, as such, afford a robust and transparent standard for permissible – and impermissible – state access to individuals' information. For example, the requirement that information is retained no longer than is necessary, as given in principle and applied by the Court below, properly informs the s 21 right. For example, the 2018 decision of the United States Supreme Court in *Carpenter* declined to hold that detailed mobile phone data held by service providers is not subject to expectations of privacy. Instead, and following its earlier holding in *Jones* that increasingly sophisticated technological means of information-gathering should not erode Fourth Amendment safeguards, the Court held such access to constitute a search on the ground that:[28]

> "Unlike the nosy neighbor who keeps an eye on comings and goings, [the service providers] are ever alert, and their memory is nearly infallible."

Sections 11(2)/31(1) and substantive divergence / procedural duplication

17. The further point that arises from the decision of the Court below and from *Alsford* is, as noted, the interpretation to be given to the "non-enforceability" provision in ss 11(2) and 31(1) of the Privacy Acts.[29]

18. The straightforward interpretation, it is submitted, is that the provision is – as noted in *Alsford* – concerned with the enforcement mechanisms under the two Acts, and not – contrary to the reasoning in *Alsford* - with the legal force of those principles. The potential separation was earlier noted by

---

28 *Carpenter v. United States*, 585 U.S. ___, 138 S.Ct. 2206 (2018) slip opinion at 16-17 and above n 4.

29 These provide that, other in respect of the enforceable right of access to personal information held by the state, the principles "do not confer on any person any [legal*] right that is enforceable in a court of law."

*The term "legal" is included in the 1993 Act but not the 2020 Act.

Blanchard J in *Hamed*, observing that the use of surveillance in a public place:[30]

> ".. should generally not be regarded as a search (or a seizure, by capture of the image) because, objectively, it will not involve any state intrusion into privacy"

and that:

> "Concern with how a law enforcement agency may use images so captured in a public place … can, if necessary, be controlled by privacy legislation or by the civil law.

19. It does not follow, however, that the two bodies of law can or should be applied separately. In addition to the points already made that the principles afford an objective and robust basis on which to determine whether there is an intrusion into privacy:

    19.1 There is otherwise a risk of procedural duplication, and even conflict. as borne out by the recent joint report and as could also be pursued by an accused person through proceedings, a Police practice can be subjected to a mandatory compliance notice or remedial orders under the Privacy Acts and fall to be considered separately under ss 21 and 30.

    19.2 The second and more significant reason to apply the principles to ss 21 and 30 is to avoid what has been termed the "balkanisation" of privacy law: that is, a separation between the law of search and seizure and the approach – and, foreseeably, the different substantive conclusions – of civil privacy law and its international antecedents, in particular as applied to government collection, retention and use of data.[31]

Privacy and tikanga

20. The further aspect, not in evidence in the present proceeding but as for example arose in the joint report, is the scope under the principles to

---

30 *Hamed v R* [2012] 2 NZLR 305, [2011] NZSC 101, [167] & n197.

31 See, for example, David Sklansky "Too Much Information: How Not to Think About Privacy and the Fourth Amendment" (2014) 102 Calif LR 1069 and Winkelmann above n 1, 17 & 20.

acknowledge and address tikanga in respect of intrusions.[32] While these necessary perspectives could also be applied under ss 21 and 30, they do further emphasise the utility of the wider contextual analysis afforded by the right to privacy.

Ensuring continued efficacy of ss 21 and 30 in the face of new technology and "third source" powers

21. The further and broader basis for the relevance of the principles, and the right to privacy, to ss 21 and 30 is that:

21.1 The effect of the increasing power, availability and ease of use of technological tools to collect, analyse and disseminate information is not only that information is ever more readily collected – both for technological reasons and, as noted by Sotomayor J in concurrence in *Jones*, because constraints of cost or civic objection are removed[33] - but also that data, however apparently innocuous, can be retained, combined, accessed and used to a greater, unprecedented and on occasion unappreciable intrusive effect.[34]

21.2 The necessary corollary of that expansion is that, as held in *Jones* and also by the Supreme Court of Canada in for example *TELUS*, a broader and contextual view of the right against unreasonable search and seizure is required to avoid the technological erosion of that right.[35]

21.3 That necessity is, in particular, driven where "third source" powers are sought to be invoked, as in the present case. In addition to the

---

32 Above n 26, 104f, canvassing both the question of intrusion and attendant whakamā and takahi mana and remedy take, utu, ea and see further Khylee Quince and Jayden Houghton "Privacy and Māori Concepts" in Nikki Chamberlain & Stephen Penk *Privacy Law in New Zealand* (3ed: 2023) 43.

33 See, as a straightforward example, that of mobile phone data held by service providers in *Carpenter* above n 28, slip at 12:

> "the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' … the retrospective quality of the data here gives police access to a category of information otherwise unknowable."

34 See, particularly, the useful historical perspective in Forcese, above n 1.

35 Above n 4 & 28 and *R v. TELUS* [2013] 2 SCR 3, [5] "Technical differences inherent in new technology should not determine the scope of protection afforded to private communications …"

general point that such powers may not cut across either a statutory scheme or, more broadly, protected rights:[36]

21.3.1 The right to privacy requires that intrusive powers be prescribed by law: while these may, conceivably, include "third source" powers, some means is needed to afford that necessary clarity;[37] and

21.3.2 More broadly, the risk is that these means are developed and exercised without general prior legislative and public consideration, as well as without approval or applicable conditions or limitations in any instant case.[38]

Relevance of context to whether s 21 applicable

22. The Court below has found, with reference to this Court's decision in *Hamed*, that the Police officer's photographing of the appellant amounted to a search within the meaning of s 21. While accepting that people in public "can have a low expectation of privacy", the Court concluded:[39]

> "It is necessary to bring to bear the fact that the photographer is a police officer … who was deliberately capturing the image for identification purposes. We consider there is a reasonable expectation that will not occur in a public place without a good law enforcement reason.
>
> … In accordance with the majority judgment in *Hamed*, the question of whether there was a search is be addressed by asking whether Mr Tamiefuna had a reasonable expectation of privacy in the circumstances in which the photos were taken. We are of the view he did. The photographs were taken at night, after he had been compelled by circumstances to leave the vehicle."

23. Before this Court, the appellant has endorsed that approach and conclusion, adding that the photographing was unjustified in the absence of necessary

---

36 *Minister for Canterbury Earthquake Recovery v Fowler Developments Ltd* [2013] NZCA 588; [2014] 2 NZLR 58, [82]; reversed, but on other grounds, *Quake Outcasts v Minister for Canterbury Earthquake Recovery* [2016] 1 NZLR 1; [2015] NZSC 27, [111]-[112].

37 See above n 27.

38 See, among many others, the observation in *Johnson v United States*, 333 US 10, 14 (1948):

> "The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate, instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."

39 Judgment under appeal, [42]-[54] (analysis of *Hamed*) and [57]-[58], **Case 22-27**.

suspicion.[40] The respondent has taken the position that as the appellant was in a public place, there was no expectation of privacy and, further:[41]

> "That enforcement of [the Land Transport Act] led to Mr Tamiefuna standing on a footpath does not point to him having any greater expectation of privacy than … a person who exits a car that has broken down."

24. As held by this Court in *Hamed* and relied upon by the Court below, the point that a photo occurred in public is not dispositive. It is also not, analytically, particularly useful. The relevance of photography in a public place, as for example put by Blanchard J in *Hamed*, is that it: [42]

> "… should generally not be regarded as a search (or a seizure, by capture of the image) because, objectively, it will not involve any state intrusion into privacy."

25. The question of whether given state conduct amounts to an intrusion into privacy will, as held by the European Court of Human Rights, depend upon context.[43] Here, two related questions arise:

    25.1 First, as to the context "in which the information … has been recorded", the relevance of the exercise of statutory powers that led to, and in practical terms enabled, the officer's photography; and

    25.2 Second, as to retention, use and processing, the relevance of the purpose and effect of that photography, which was for uploading into the NIA database, and not for any purpose related to the stop or any immediate circumstance.

---

40 Appellant submissions, [25]-[45], citing among others *R (Wood) v Metropolitan Police Commissioner* [2009] 4 All ER 951 (EWCA) and also the IPCA/Commissioner joint report above n 26. See, particularly, the observation of Collins LJ in *Wood*, [98]-[100] noting the ECHR requirement that intereference with privacy must be according to law and concluding:

> "... it is plain that the last word has yet to be said on the implications for civil liberties of the taking and retention of images in the modern surveillance society. This is not the case for the exploration of the wider, and very serious, human rights issues which arise when the State obtains and retains the images of persons who have committed no offence and are not suspected of having committed any offence."

41 Respondent submissions, [75] and [70]-[81], including with reference to Canadian and United States authority that what one "knowingly exposes to the public" is not protected.

42 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 [167].

43 *Marper*, above at n 24.

Relevance of statutory powers

26. The practical effect of the exercise of the Land Transport Act random vehicle stop power was not only that the vehicle in which the appellant was a passenger was stopped by Police; the driver found to be unlicensed; and the car impounded, as provided for under that Act, but also that:

    26.1 The stopping Police officer looked into the interior of the vehicle and asked for the passengers' particulars, which they gave;

    26.2 Having impounded the car, the officer was able to take photographs of the passengers on the roadside as they waited for a tow truck and upload the photographs and particulars into the NIA database;[44] and

    26.3 The NIA database then retained and disseminated that information in a searchable manner.

27. The exercise of a statutory power, even if only with indirect effect upon a party such as the appellant, is a relevant factor to the privacy analysis. The particular issue – as here – of steps consequent on a vehicle stop has also arisen at length in other jurisdictions. Notably:

    27.1 The United States Supreme Court has repeatedly addressed fourth amendment issues arising from the conduct of traffic stops and permitted steps consequent on such stops. The Court has held that:[45]

        27.1.1 Under the fourth amendment, warrantless traffic stops are permissible on the grounds of a reasonable and articulable suspicion of criminal activity; but

        27.1.2 The stop may take only such time as is required to effectuate the purpose relied upon; and

        27.1.3 Investigative steps into any other matter are permissible only with "independently supported reasonable suspicion" of that matter: in the leading case, *Rodriguez*, the Court found that police could lawfully stop the appellant to investigate why he

---

44 Judgment under appeal [8], **Case 12**.

45 *Rodriguez v United States*, 575 US 348 (2015),

had swerved out of a line of traffic but the use of a drug sniffer dog required such independent grounds.

27.2 The position is similar in Canada: because random traffic stops can be justified by appropriate purposes – such as enforcement of vehicle licensing, safety and/or sobriety – those powers must be exercised vigilantly and within those purposes: they may not give rise to an "unfounded general inquisition".[46]

Rights-consistent interpretation of s 30 of the Evidence Act 2006

28. The interpretation of s 30 is addressed last here, notwithstanding that it is the point on appeal, because – as also in the decision of the Court below – it is consequent on the points already addressed.

29. The parties have addressed the correct interpretation of s 30 and, particularly, of the broad requirements in s 30(2)(b).[47] It is necessary to supplement those careful and detailed submissions only in brief terms.

30. The first is that, at least in those cases in which the evidence in issue is found to have been obtained in breach of s 21 or another human rights obligation, s 30 should be interpreted so as to afford an effective remedy for that breach of right.[48] As is well-settled, an effective remedy must both vindicate the right of the individual and avoid recurrence.

31. The result is not as simple as requiring exclusion of evidence in every such case:

---

46 *R v Mellenthin* [1992] 3 SCR 615, 624 and see for example *R v Nolet* [2010] 1 SCR 851 upholding a search of a truck driver's duffel bag as part of the "regulatory" search but a wider "inventory" search as unlawful; though see also the discussion of difficulties in drawing that distinction in T Skolnik "Policing in the Shadow of Legality: Pretext, Leveraging, and Investigation Cascades" (2023) 60 Osgoode Hall LJ 505.

47 Section 30(2)(b) provides:

> "The Judge must– ...
>
> (b) if the Judge finds that the evidence has been improperly obtained, determine whether or not the exclusion of the evidence is proportionate to the impropriety by means of a balancing process that gives appropriate weight to the impropriety and takes proper account of the need for an effective and credible system of justice."

and see, respectively, appellant submissions at [60]ff and respondent at [98]ff.

48 See, particularly art 2(3)(a) ICCPR, which requires states parties:

> "To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity ..."

31.1 While exclusion is mandatory in respect of evidence obtained by torture and, similarly, the right to a fair trial, other rights – including, as here, the s 21 and art 17 rights – can be qualified by compelling contrary interests or otherwise remedied;[49] and

31.2 Other than in respect of absolute rights,[50] such a balanced interpretation is required by s 30 and by s 4 of the Bill of Rights Act.

32. What the obligations in respect of effective remedy do require, however, is robust vindication and non-recurrence. The analytical and empirical material put by the appellant – both as prepared by appellant counsel and as set out in Law Commission studies – raise questions as to whether s 30 is in practice interpreted in that manner: [51]

32.1 The statistical indications in the appellant's table and the Law Commission study – in particular, the rate of exclusion – may suggest a less stringent approach compared to practice in Canada; and

32.2 What is in any case apparent from the appellant's data and from the most recent Law Commission study is a lack of clarity in or, at least, uneven engagement with certain of the factors given in s 30.

---

49 See the useful survey of differing positions among states parties to the ICCPR, including discussion of the position prior to s 30/ *R v Shaheed* [2002] 2 NZLR 377 (CA) and since, in respect of evidence obtained in breach of privacy, Dimitrios Giannoulopoulos *Improperly Obtained Evidence in Anglo-American and Continental Law* (Hart, 2019), 219ff. The leading Canadian scholar Kent Roach has also advocated for a "structured" approach in which the state may justify alternative remedies as alternatives to exclusion: see, particularly, "Reclaiming Prima Facie Exclusionary Rules in Canada, Ireland, New Zealand, and the United States: The Importance of Compensation, Proportionality, and Non-Repetition" (2020) Manitoba L J 1, 46-47.

50 See *Kim*, above n 2 (statutory power not discretionary in respect of absolute obligations).

51 In addition to the detailed analysis set out in the appellant's submissions, the statistical analysis, also cited for the appellant, in Law Commission *Te Arotake Tuatoru i te Evidence Act 2006 | The Third Review of the Evidence Act 2006* (Issues Paper 50, 2023) [7.40]:

> "[S]ection 30 decisions more often lead to admission of improperly obtained evidence, particularly where physical evidence is involved (as opposed to defendants' statements). The importance of the evidence to the prosecution case and the seriousness of the offence are often treated as significant - and sometimes determinative - factors."

and cf, for example, the breakdown of exclusion decisions and cited grounds in Benjamin Johnson, Richard Jochelson & Victoria Weir "Exclusion of Evidence under Section 24(2) of the Charter Post-*Grant* in the Years 2014-2017: A Comprehensive Analysis of 600 Cases" (2019) 67 Crim L Q 56, 89 and also (at 56-57) average exclusion rate of approximately seventy percent at trial. The appellate exclusion rate in the Canadian sample was comparable to that put by the appellants, but – on the Law Commission data – from a lower exclusion rate at first instance.

33. The effective remedy obligation – and the objects of vindication and non-recurrence – may afford greater robustness to the s 30 assessment:

33.1 The first, and more broadly framed, point is that stressed by members of the Court in *Hamed*, consideration of "the need for an effective and credible system of justice" in s 30(2)(b) proceeds, at least in part, from the starting point that impropriety in respect of evidence itself undermines the rule of law.[52] Put short, rigorous engagement with s 30(2)(b) serves that purpose.

33.2 The second is that the effective remedy obligation affords – and requires – a structured approach to those rule of law concerns. In particular, the emphasis upon non-recurrence requires consideration of both whether the breach was itself part of a systemic practice and whether admission of evidence permits or, at least, does not prevent future such actions.[53] That is consistent with the concern for the "longer-term" expressed in *Hamed* and in *Grant*.[54]

B Keith / A de Joux
Counsel for the Commissioner

---

52 See *Hamed v R* [2012] 2 NZLR 305, [2011] NZSC 101 at [27], [38] & [62] per Elias CJ (though dissenting as to result): need for authorisation "part of the rule of law" and "meets rule of law values of certainty and predictability" and (concurring on the particular point) "an effective and credible system of justice [under s 30(2)(b)] is one that gives substantive effect to human rights and the rule of law"; [187] per Blanchard J:

> "... the fact of the breach means that damage has already been done to the administration of justice. The courts must ensure in the application of s 30 that evidence obtained through that breach does not do further damage to the repute of the justice system ..."

citing *R v Grant* 2009 SCC 32, [2009] 2 SCR 353, [68]–[69]; and[230] per Tipping J:

> "The admission of improperly obtained evidence must always, to a greater or lesser extent, tend to undermine the rule of law. By enacting s 30 Parliament has indicated that in appropriate cases improperly obtained evidence should be admitted, but the longer-term effect of doing so on an effective and credible system of justice must always be considered."

53 See, for example, Roach above n 49 and also Veenu Goswami "Breaking the Purposive Barrier: Embracing Non-Repetition as a Guiding Principle for Subsection 24 (2) of the Charter" (2018) 51 UBC Law Rev 289.

54 Above n 52.