ALEC DUNCAN

"WELL-MEANING, BUT WITHOUT UNDERSTANDING":

ARE WARRANTLESS POLICE INFORMATION REQUESTS TO THIRD PARTIES CONTRARY TO SECTION 21 OF THE NEW ZEALAND BILL OF RIGHTS ACT 1990?

Submitted for the LLB (Honours) Degree

FACULTY OF LAW
VICTORIA UNIVERSITY OF WELLINGTON

2016

Abstract:

Early in their investigations, it is common practice for police to make warrantless requests to banks, telecommunications providers, power companies and other service providers. In making these requests, the police hope to obtain information about their suspect (such as financial transaction records or call records) which will assist the police in obtaining search warrants. New Zealand courts have dismissed claims that requests constitute an unreasonable search or seizure per s 21 of the New Zealand Bill of Rights Act 1990, holding that principle 11(e)(i) of the Privacy Act 1993 authorises both the disclosure and use of information. This paper argues that such an approach does not reflect the first principles approach advocated in Hamed v R *and by the Canadian Supreme Court because it gives insufficient weight to privacy interests, to the fact that disclosure of personal information is often compulsory when using services and to the nature of the information sought. It concludes that such requests are thus searches or seizures and, not being authorised by any positive law (the Privacy Act in particular), will be unreasonable in most cases. This paper argues that police should instead utilise the production order regime in the Search and Surveillance Act 2012.*

Key words: New Zealand Bill of Rights Act 1990, s 21; Privacy Act 1993, principle 11(e)(i); information requests; *Hager v Attorney-General*; *R v Alsford*.

Contents

The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding.[1]

I Introduction

A Police Practice when Requesting Information from Agencies

It is one thing for the police to knock on your door and request access to your computer, papers and other private information; it is another thing entirely when the police make the same request of your bank or power company. But that is what the police do on a regular basis, most notably in *Hager v Attorney-General*.[2] Mr Hager, a noted investigative journalist, included in his book material obtained from a hack of the Whale Oil Blog servers.[3] The police ultimately decided to treat him as "an uncooperative witness rather than a suspect".[4] To further their investigation, the police sent information requests to various banks, to TradeMe, Spark New Zealand, Vodafone, Air New Zealand and Jetstar.[5] Only Westpac Bank complied, providing "detailed information about Mr Hager's bank account".[6] The other agencies asked the police to obtain a production order.[7]

In making their requests, the police relied on a generic form which stated that their request relied upon Information Privacy Principle 11(e)(i) of

---

1 *Olmstead v United States* 277 US 438 (1928) at 479, per Brandeis J (dissenting).

2 *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523.

3 At [10] and [12].

4 At [14]; *Hager v Attorney-General* Written Submissions for the Applicant CIV 2014-485-11344 at [2.33].

5 *Hager* Written Submissions for the Applicant, above n 4, at [2.30].

6 At [2.31].

7 At [2.54], [2.57], [2.62] and [2.66].

the Privacy Act 1993 ("IPP11(e)(i)") and were not urgent.[8] Under that principle, agencies holding personal information:[9]

> … shall not disclose the information … unless the agency believes, on reasonable grounds,—
>
> …
>
> (e) that non compliance is necessary—
>
> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including … the prevention, detection [and] investigation … of offences.

The purpose of the form's use is that the information should be disclosed because the police need it to investigate an offense.

Had the police, faced with the agencies' reticence, chosen to obtain production orders, they would have had to show, pursuant to the Search and Surveillance Act 2012 ("the SSA") that they had:[10]

> … reasonable grounds—
>
> (a) to suspect that an offence has been committed … ; and
>
> (b) to believe that the documents sought by the proposed order—
>
> (i) constitute evidential material in respect of the offence; and
>
> (ii) are in the possession or under the control of the person against whom the order is sought …

Production orders allow police to compel the recipient to hand over the documents to police or disclose who possesses them.[11]

This investigative technique risks that investigation might fall afoul of s 21 of the New Zealand Bill of Rights Act 1990 ("NZBORA") which guarantees "the right to be secure against unreasonable search or seizure,

---

8 See *Hager v Attorney-General* Key Evidence Bundle Volume 4: Key Police Disclosures CIV 2014-485-11344 at PD 4/558–565.

9 Privacy Act 1993, s 6, cl 11(e)(i).

10 Section 72.

11 Search and Surveillance Act 2012, s 75(1).

whether of the person, property, or correspondence or otherwise." According to *Hamed v R*, resolution of a s 21 claim requires the determination of two issues: first, whether police receipt of information is a search or seizure; and second, whether such actions are unreasonable.[12]

This paper will adopt this structure to analyse the issues arising from such requests. Moreover, since Canadian and United States jurisprudence reflect the same structure and principles as New Zealand jurisprudence, this paper will derive assistance from those jurisdictions.[13]

This paper asks whether police receipt and use of information resulting from a Warrantless Request for a Customer's Information ("WRCI") constitutes an unreasonable search or seizure per s 21 of NZBORA. There are several points underlying this term that should explained. First, enforcement agencies, such as the police, undertake WRCIs.[14] Secondly, WRCIs are directed to "agencies" (any person or company, whether public or private sector) in respect of personal information (information about an identifiable person).[15]

B The Approach to s 21

1 Establishing a search or seizure

A claim under s 21 must first establish that the state has conducted a search or seizure. Courts have distinguished between searches and seizures, holding the former to be "an examination of a person or property" and the latter to be "a taking of what is discovered". This paper, however, argues that the

---

12 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [162].

13 For Canada, see *Hunter v Southam Inc* [1984] 2 SCR 145; and *R v Wise* [1992] 1 SCR 527, cited with approval in *Hamed*, above n 12, at [161] and [163]; for the United States, see *Katz v United States* 389 US 347 (1967).

14 "Enforcement officer" is defined in the Search and Surveillance Act 2012, s 3(1).

15 See "Agency" and "Personal Information" as defined in the Privacy Act 1993, s 2(1).

distinction is neither useful nor possible when examining WRCIs,[16] despite some cases treating WRCIs as being one or the other.[17]

None of the forgoing affects a first principles approach to s 21. Blanchard J observed in *Hamed* that NZBORA's purpose was to extend the prohibition against unreasonable search and seizure beyond "physical acts of trespass" to cases in which there is an unjustified "state intrusion on an individual's privacy.[18] A breach of s 21 is predicated on whether police actions invade a complainant's reasonable expectations of privacy.[19]

Part II analyses the New Zealand courts' approaches to WRCIs. There is more than 20 years of New Zealand jurisprudence which holds, first, that police receipt of information is lawful if agencies release it pursuant to IPP11(e)(i); and secondly, that complainants cannot use the tort of breach of confidence to prevent third parties from disclosing their iniquitous behaviour to the police.

Following an examination of the approach to unreasonable search and seizure espoused in *Hamed v R* and by Canadian and United States jurisprudence, Part III argues that the approach established in Part II is inconsistent with the privacy interests which underlie s 21.

2 Unreasonableness

The second question under a s 21 analysis relies on a fact-specific policy analysis as to whether the complainant's reasonable expectations must

---

16 See *Hamed*, above n 12, at [161], citing *R v Jefferies* [1994] 1 NZLR 290 (CA) at 300.

17 For WRCIs as a search, see *S v Police* (2002) 22 FRNZ 28 (HC) at [21]; for WRCIs as a seizure, see *R v Sanders* (1994) 12 CRNZ 12 (CA) at 35.

18 *Hamed*, above n 12, at [161].

19 At [163].

give way to the state's interest in enforcing the law.[20] Part IV assesses whether New Zealand courts should treat WRCIs as lawful or reasonable. It argues that, since there is no positive law authorising WRCIs, they are prima facie unreasonable. Moreover, the approach taken in New Zealand is inconsistent with society's desire to keep such information private from those we do not believe will view it.[21]

This paper concludes that individuals retain a reasonable expectation of privacy in information communicated to third parties and that WRCIs thus constitute a search or seizure. It also concludes that WRCIs are unreasonable as no statutory authority authorises them and because the SSA's production order regime provides adequate authority for activities almost identical to WRCIs. This paper argues that production orders should be the legal standard for obtaining information from agencies because of the production order regime's similarity to WRCIs, along with the judicial oversight required to issue orders.

As there is no positive authority for WRCIs, this paper will not analyse whether WRCIs are a justified limitation on s 21 per s 5 of NZBORA.[22] Moreover, given the fact-specific nature of the inquiry, this paper will not examine whether such information should be excluded under s 30 of the Evidence Act.

---

20 See for example, *Hamed*, above n 12, at [161], citing *Hunter*, above n 13, at [17]; *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA) at 407; and *Jefferies*, above n 16, at 301–302.

21 See for example *Hager v Attorney-General* Key Evidence Bundle Volume 1: Applicant's Affidavits CIV 2014-485-11344 at [160]–[161]; and Office of the Privacy Commissioner "Transparency Reporting Trial Aug–Oct Full Report" (18 February 2016) Privacy Commissioner <www.privacy.org.nz> at [3]–[5].

22 See for example *Hamed*, above n 12, at [162]; and *Cropp v Judicial Committee* [2008] NZSC 46, 3 NZLR 774 at [33].

II New Zealand Jurisprudence on WRCIs

R v Sanders represents an early approach to WRCIs from which later cases departed. In *Sanders*, police approached various agencies with an invalid search warrant for information about suspected cannabis cultivation; the agencies voluntarily provided the documents sought.[23] Fisher J held that the police require legal justification (relevantly, a search warrant or the agency's consent) if their actions infringe a right of interest.[24]

The subject's consent is required if the release would breach a duty of confidence between the subject and the agency or would infringe upon the subjects property rights or personal dignity.[25] If none of these are implicated, the agency may validly consent to the information's release.[26]

As the following analysis shows, later courts have used Fisher J's exception as the basis for holding that WRCIs are lawful because they infringe no property or confidentiality interests.

A Principle 11 of the Privacy Act

IPP11(e)(i) allows agencies to disclose personal information where not doing so would prejudice the maintenance of the law. Courts post-*Sanders* have held that releasing information pursuant to IPP11(e)(i) is proof that the agency's consent is effective for the purposes of the *Sanders* exception. In agreeing with submissions that WRCIs are not unlawful for law enforcement purposes,[27] courts have implied that the police can rely on an agency's release as proof that IPP11(e)(i)'s conditions are satisfied and that release of the

---

23 *Sanders*, above n 17, at 16–18.

24 At 32.

25 Ibid.

26 Ibid.

27 *R v Thompson* (1995) 13 CRNZ 546 (HC) at 553 [*Thompson* (1995)]; *R v Harris* [2000] 2 NZLR 524 (CA) at [10]; and *R v Thompson* [2001] 1 NZLR 129 (CA) at [54] [*Thompson* (2001)].

information would not infringe the subject's rights or interests.[28] This presumption does not apply where police have "reason to believe that the disclosure would be unlawful."[29]

B Iniquity and Agencies' Duties of Confidence

Complainants have attempted to attack agencies' disclosures on the basis that they owe customers a duty of confidence. A duty of confidence has been summarised thusly as: [30]

(1) concerning confidential (not publically known) information;
(2) arising when that information is imparted to another under circumstances implying that the recipient will not disclose the information;
(3) being breached by the recipient if they make unauthorised disclosure or use of the information; and
(4) being qualified a legitimate public concern or other just cause for disclosure.

Where such a duty attaches to the information disclosed, release thereof infringes upon a subscriber's interests.[31]

In *R v H*, the defendant (H) sought to exclude documents, provided to police by H's accountant (D), which showed that H had circumvented fishing quota reporting requirements by bribing a fisheries officer.[32] The Court, applying the rule in *Gartside v Outram*, held that H could not rely on an employer–employee duty of confidence to challenge the lawfulness of D's

---

28 See *Thompson* (1995), above n 27, at 553.

29 *Harris*, above n 27, At [10].

30 *Laws of New Zealand* Tort (online ed) at [326]–[329]; for banks' duties of confidence, see *Tournier v National Provincial and Union Bank of Enland* [1924] 1 KB 461 (CA); *Hunt v A* [2007] NZCA 332, [2008] 1 NZLR 368 at [65].

31 *Sanders*, above n 17, at 32.

32 *R v H* [1994] 2 NZLR 143 (CA) at 145 and 146.

disclosure because "there is no confidence as to the disclosure of iniquity".[33] The same reasoning was applied in *R v Cox* and *R v Javid*, which both concerned the use of Vodafone's network to arrange drug manufacture and distribution.[34] Though users of telecommunication services are entitled to expect that the "operator would maintain confidentiality",[35] there was nothing "wrong or inappropriate" about Vodafone's provision of information to the police because the appellants used Vodafone's network to conduct criminal activities, the exposure of which was a legitimate public concern.[36]

C The Use of s 21 of NZBORA

Early on, courts recognised that distinctions must be drawn between the actors involved. In *Sanders*, the Court distinguished between agencies' searches for information pursuant to requests and the release thereof to police. Police do not engage s 21 until they receive information because agencies are lawfully entitled to search through information provided to them.[37] The same was true in *R v H*, in which the Court held that s 21 was not engaged when H's accountant initially disclosed H's bribery to police but was engaged when police asked H's accountant to continue to supply them with information because D's actions in the latter case could be seen to be those of a "government agent".[38]

S v Police grappled explicitly with the impact of WRCIs on reasonable expectations of privacy. S challenged the admissibility of a letter he sent to Children and Young Persons Service (CYPS) alleging criminal activities

---

33 At 148, citing *Gartside v Outram* (1856) 26 LJ Ch 113 at 114; see limb (4) above regarding the qualification of duties of confidence.

34 *R v Cox* (2004) 21 CRNZ 1 (CA) at [1] and [6]; *R v Javid* [2007] NZCA 232 at [2] and [27]–[28].

35 *Cox*, above n 34, at [33].

36 At [69]; and *Javid*, above n 34, at [45(c)].

37 *Sanders*, above n 17, at 35.

38 *R v H*, above n 32, at 147 and 148.

rendering a woman unfit to care for her children.[39] The police requested and received the letter from CYPS as part of an investigation against S.[40] Applying the concept of reasonable expectations of privacy to Fisher J's agency consent exception in *Sanders*,[41] Pankhurst J held that the police receipt was lawful because none of S's rights or interests where infringed as a statutory information-sharing scheme between the police and CYPS meant that S could not reasonably expect that his letter would not be disclosed.[42]

D R v Alsford*: Departing from this Jurisprudence?*

More recently, in *R v Alsford*, there are signs of a new approach emerging. *Alsford* concerned a request for power consumption information based on a tip-off relating to cannabis cultivation.[43] Ellen France P expressed doubts that *Thompson* (2001) was correct to hold that IPP11(e)(i) allows information disclosure for law enforcement purposes.[44] Her Honour also expressed support for the proposition that the production order regime contained in the SSA should have been utilised instead of a WRCI.[45]

However, there is no ratio on this point as French J dissented, arguing that *Thompson* (2001) should be followed.[46] Winkelmann J, though concurring in result, expressed no view on the matter.[47] Moreover, the case is currently on appeal to the Supreme Court, meaning that the President's remarks

---

39 *S v Police*, above n 17, at [5].

40 At [8].

41 See [16] and [17], citing *R v Sanders* (1994) 12 CRNZ 12 (CA) at 36.

42 See *S v Police*, above n 17, at [21].

43 *R v Alsford* [2015] NZCA 628 at [8].

44 At [50], citing *Thompson* (2001), above n 27, at [54].

45 *Alsford*, above n 43, at [53]–[54].

46 At [90].

47 At [94]ff.

may be approved or disapproved or that the Court may set down a coherent approach to WRCIs.

E Conclusions on the approach

The preceding discussion shows that New Zealand courts have approached the issue of WRCIs without providing any coherent approach. Though courts have variously recognised that WRCIs could amount to a search or seizure, they ultimately concluded that IPP11(e)(i) or the rule in *Gartside* overrode s 21 concerns.

Even in *Alsford*, the most recent case on the subject, the judges (as in the aforementioned cases) seemed to treat WRCIs as a separate species of police action. However, there is, arguably, little practical privacy distinction between entering a person's home and finding a power bill or bank statement and asking an agency to provide that material. In both cases, the police obtain information which few people would otherwise have access to.

III When will WRCIs Amount to a Search or Seizure?

The problem with the aforementioned approaches is that they do not reflect s 21's first principles. This Part will set out the approach taken in the leading Supreme Court decision of *Hamed v R* as to when state actions constitute a search or seizure. It will then consider the same question in light of the Canadian and United States' approaches. Since s 21 of NZBORA, s 8 of the Canadian Charter and the Fourth Amendment to the United States Constitution are aimed at protecting privacy interests against state intrusion, we would expect similar approaches between the jurisdictions. This is not the case. Instead, New Zealand's courts rely on generic factors – such as the disclosure of information to third parties – to militate against a finding that WRCIs implicate reasonable expectations of privacy and thus against a finding that s 21 is triggered.

This Part concludes that Canada's approach better reflects the importance people attach to privacy by focusing on the nature of the information and its relationship with other private information rather than on the disclosure to a third party. Canadian courts are better placed than New Zealand courts to protect privacy interests from state intrusion. Given that information held by agencies can be lawfully released on request, the latter's approach seriously limits the scope of privacy in an age where more and more personal information is held by third parties.

A The Approach Taken to Search and Seizure in Hamed

Hamed represents the current New Zealand approach to s 21.[48] The case concerned the admissibility of covert video surveillance obtained pursuant to warrants incapable of authorising such surveillance.[49] The majority held that the police surveillance which took place on private land constituted an unreasonable search under s 21 because, absent valid warrants, the police actions amounted to a trespass, rendering their activities unlawful.[50]

Though the judges delivered separate opinions, the Court of Appeal in *Lorigan v R* concluded that the majority in *Hamed* supported Blanchard J's statements as to the circumstances under which state actions amount to a search or seizure.[51] O'Regan P noted that McGrath J (who expressed no opinion on that point in *Hamed*) had "expressed similar views [as Blanchard J in *Hamed*]" in *R v Ngan* and that if his Honour had expressed a view in *Hamed*, "it would have been consistent with that of Blanchard J."[52]

---

48 Much assistance has been derived from Samuel Beswick "Perlustration in the Pathless Woods: *Hamed v R*" (2011) 17 Auckland U L Rev 291; and Harriet Bush "The Video Camera Surveillance (Temporary Measures) Act 2011: An Unprecedented Licence to Search?" (2013) 44 VUWLR 221.

49 *Hamed*, above n 12, at [92]–[107].

50 At [171] and [175] per Blanchard J and [217] per Tipping J.

51 *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22].

52 See *Hamed*, above n 12, at [263] per McGrath J; *Lorigan*, above n 51, at [18]; see also *R v Ngan* [2007] NZSC 105, [2008] 2 NZLR 48 at [104] and [107].

In basing his definition of what types of actions constitute a "search" or "seizure" on s 21's first principles, Blanchard J (writing for himself and Gault J) agreed with the Chief Justice that s 21 "reflects an amalgam of values", including privacy.[53] Blanchard J likewise agreed with Elias CJ that s 21 concerns instances where "police activity invades a person's reasonable expectations of privacy".[54] However, his Honour disagreed that s 21 *guarantees* reasonable expectations of privacy against state intrusion.[55] As such, whilst Elias CJ's analysis strongly implies that *any* state intrusion into a person's reasonable expectations of privacy is unreasonable and therefore a breach of s 21,[56] Blanchard J's analysis reflects the possibility that such an intrusion might, nonetheless, be reasonable.[57]

To determine when a person's reasonable expectations of privacy might be invaded, his Honour adopted the two step test from *United States v Katz*, holding that a reasonable expectation of privacy exists if:[58]

(1) the complainant subjectively expected privacy in the circumstances; and

(2) that expectation "was one that society is prepared to recognise as reasonable".

Blanchard J disagreed with Elias CJ on the latter point. For Blanchard J, the fact that the surveilled actions took place in public was relevant to whether the

---

53 *Jefferies*, above n 16, at 302, cited in *Hamed*, above n 12, at [161].

54 At [163], citing *Wise*, above n 13 at 533.

55 *Hamed*, above n 12, at [161]; compare with Elias CJ at [10].

56 At [10] per Elias CJ.

57 At [162]; for the two-step test, see above n 12.

58 *Hamed*, above n 12, at [163], citing *Katz*, above n 13 at 361.

state intruded upon a person's reasonable expectations of privacy, whereas Elias CJ thought that factor was irrelevant.[59]

Acceptance by the majority in *Hamed* of the strong links between s 21 and the protection of privacy reflects the ongoing divorce of the common law's trespass-focused jurisprudence from s 21's privacy-based understandings of search and seizure.[60] Commenting on *R v Jefferies*, Optican observed that, by taking North American privacy values as part of s 21's first principles, New Zealand's courts opened s 21's application to "a wide range of police investigative activities" some of which are "conducted far from the individual" and thus involve "no material intrusion into legally protected space."[61] Our courts have thus become increasingly clear that whilst privacy and proprietary interests are the touchstones of s 21, the latter's absence will not necessarily be fatal to a claim under s 21.

Applying Blanchard J's test to information held by agencies, it is arguable that people expect that such information will be held in confidence, as it often reveals highly personal information about identifiable individuals.[62] It is further arguable that the Privacy Act, by prescribing particular exceptions to the requirement of non-disclosure, acts as legislative confirmation that such a belief is reasonable, except where investigative interests (such as urgent situations) are paramount.

However, judicial opinion has construed this exception so broadly that almost any disclosure of information pursuant to a WRCI falls within the *Sanders* agency consent exception because it implicates no privacy interests. Realistically therefore, no matter how much a person expects that an agency

---

59 *Hamed*, above n 12, at [167]–[168]; compare with Elias CJ at [12].

60 See also *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [63].

61 Scott Optican "What is a "Search" under s 21 of the New Zealand Bill of Rights Act 1990? An Analysis, Critique and Tripartite Approach" [2001] NZ L Rev 239 at 243.

62 See for example *Hager v Attorney-General* Key Evidence Bundle Volume 1: Applicant's Affidavits CIV 2014-485-11344 at [160]–[161].

will not disclose their information, the courts will not hold this expectation to be reasonable. The rest of this Part argues that the courts are not correct to hold that such expectations are unreasonable in respect of WRCIs.

B Conceptualising the Issues of Applying Hamed *to WRCIs*

Any analysis of an expectation's reasonableness must not conflate the two issues which WRCIs raise. The first is whether people lose a reasonable expectation of privacy because they communicate information to a third party. This question is important because there can be no blanket rule that *all* third parties owe a person privacy or confidence in information communicated to, or received by them. This would run contrary to well-established law that the public nature of an observed action diminishes or destroys the subject's reasonable expectations of privacy therein.[63] Regarding breaches of confidence, courts have held that a third party who views an occurrence in public is under no duty of confidence to the subject.[64]

If the first issue is answered in the negative, the second issue is whether that answer would be different if the information concerned the subject's wrongdoing. This second point is important because, in many cases, the police approach agencies before they have concrete evidence to suspect the subject of wrongdoing or where there is no allegation of wrongdoing.[65] If the information's disclosure of wrongdoing has no impact on the first issue, then it ought to follow that the answer to the second issue would not be different if the information did not concern the subject's wrongdoing.

---

63 For the former, see *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [119] and [164] per Gault and Blanchard JJ and at [249]–[250] and [260] per Tipping J; and for the latter, see *Hamed*, above n 12, at [167]–[168] per Blanchard J.

64 *P v D* [2000] 2 NZLR 591 (HC) at [17].

65 See for example *Alsford*, above n 43, at [36]; and *Hager*, above n 2, at [14].

C The Effect of Communicating Information to Third Parties

1 The fact of disclosure: the United States' "third party doctrine"

The corollary of the *Katz* test is that a person cannot normally reasonably expect privacy regarding information they communicate to third parties.[66] *United States v Miller* articulated the rationale for this "third party doctrine" as being that a complainant "*takes the risk*, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[67] By assuming that risk, complainants evince a lack belief that the information is private – after all, if one desires to keep information private, why would one communicate it to another person?[68]

The doctrine has been criticised as anachronistic and antiquated – ill-suited to an age "in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[69] A more fundamental problem is that so many services require us to divulge personal information as a condition of use that the private space in which information can inhabit has been much reduced.

Marshall J in *Smith v Maryland* argued that "it is idle to speak of *'assuming' risks* in contexts where, as a practical matter, individuals have no realistic alternative".[70] This pronouncement implicates situations where use of services compels us to divulge personal information – the situations in *Thompson* (2001), *Cox* and *Javid* spring to mind. Such information is not divulged by complainants; rather, they are collected as a consequence of their use of a service (financial transaction records are similar).

---

66 Lucas Issacharoff and Kyle Wirshba "Restoring Reason to the Third Party Doctrine" 100 (2016) Minn L Rev 987 at 987.

67 At 991, citing *United States v Miller* 425 US 435 (1976) at 443 (emphasis added).

68 At 995.

69 *United States v Jones* 132 S Ct 945 (2012) at 957 per Sotomayor J, concurring..

70 *Smith v Maryland* 442 US 735 (1979) at 750 (emphasis added).

There is New Zealand authority supporting the proposition that a person's consent is only effective if they have the capacity to refuse. *Cropp v Judicial Committee* concerned the validity of random drug-testing rules created by New Zealand Thoroughbred Racing pursuant to the Racing Act 2003.[71] Ms Cropp, a jockey, tested positive for banned substances following a race.[72] The Court observed that the rules mandating the tests were amenable to review under s 21 because the NZTR was "exercising a public function".[73] On the point of consent, the Court held that Ms Cropp's consent to be tested was not voluntarily given because consent was a precondition of her participation; hence, she had no real choice: consent or be barred from her profession.[74]

Though consent in *Cropp* went to the reasonableness of the search, Harker argues convincingly that, though a search by consent is still a search "in the ordinary sense of the word", such searches cannot be held to affect reasonableness if reasonable expectations of privacy form the basis for whether there has been a search.[75] Essentially, Harker's categorisation relies on the same thesis as the third party doctrine: if a person voluntarily reveals information to another, it is hard to conclude that they desired to keep it private.[76] If no reasonable expectations of privacy are implicated, there is no search.

However, *Cropp* is not readily applicable to WRCIs. Unlike the NZTR, banks and (most) other non-public agencies do not exercise public functions as their rules and policies are not delegated legislation.[77] Their acquisition of

---

71 *Cropp v Judicial Committee* [2008] NZSC 46, 3 NZLR 207 at [1].

72 At [4].

73 At [18].

74 At [22].

75 Christopher Harker "Consent Searches and Section 21 of the New Zealand Bill of Rights Act 1990" (2011) 9 NZJPIL 137 at 147 and 152.

76 At 152.

77 Compare with *Cropp*, above n 71, at [1].

subscriber information cannot trigger s 21. The only relevant body to which s 21 applies is the police.[78] A complainant's argument against the police based on an agency's disclosure would have to rely, indirectly, on a lack of consent: agencies cannot consent on behalf of subjects to release information to whose collection, per *Cropp*, the subjects never consented.[79]

This argument is highly theoretical and has, apparently, never been applied in New Zealand. Even the most proximate Canadian case, *R v Cole*, is distinguishable because the compulsion used to force Mr Cole to surrender his school-issued laptop was authorised by statute.[80] The lower constitutional standard required for the school's seizure pursuant to the Education Act 1990 meant that warrantless seizure allowed the police to circumvent the constitutional protection of private information contained in s 8 of the Canadian Charter.[81]

Any argument in favour of *Cole*'s applicability to WRCIs would turn on two points. First, that there is little to distinguish the compulsion used in each case. Third party agencies, though not compelling disclosure by statutory means, require it as a condition of service. The effect is the same in both cases: the subject discloses information when they might not have otherwise. The second argument is that, though agencies do not exercise public powers, they collect, hold and release information pursuant to the Privacy Act's requirements and the burden of responding to WRCIs lies upon them. In making WRCIs with minimal evidential information, the police can effectively circumvent the constitutional protection of information embodied in s 21 by relying on agencies to undertake the impossible task of determining whether IPP11(e)(i)'s requirements are met.

---

78 See New Zealand Bill of Rights Act 1990, s 3(a).

79 See above n 74.

80 *R v Cole* [2012] 3 SCR 43 at [62].

81 At [66] and [69].

However, one important development since *Cropp* is the enactment of the Search and Surveillance Act 2012 which states that searches undertaken by consent are unlawful if "consent [is] given by a person who does not have authority to give that consent."[82] This, along with the requirement that officers requesting searches advise consenters of their right to refuse,[83] is aimed at ensuring that consent is fully informed, in a manner similar to *Cropp*.[84]

Various authors argue that the consenter must have actual, rather than apparent authority to consent.[85] However, the SSA cannot confer actual authority on agencies: the SSA cannot be used to provide the consensual capacity which it requires; that must be ascertained from other factors. McMullan argues that those factors may include the relationship between the parties and the space being searched.[86] We should thus examine the relationship between the agency and the subject – this is the approach taken by the Canadian Supreme Court to WRCIs.

2 The context of disclosure: the Canadian approach

The Canadian Supreme Court has rejected the United States' jurisprudence. In *R v Schreiber*, the Canadian Federal Department of Justice requested that Swiss authorities seize the appellant's Swiss bank records.[87] The case was dismissed because s 8 of the Canadian Charter is not engaged by searches conducted pursuant to foreign law by foreign authorities.[88] However,

---

82 Search and Surveillance Act 2012, s 94(c).

83 Section 93.

84 Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis, Wellington, 2015) at [18.32.16].

85 See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [3.97]–[3.98]; Sam McMullan "Third Party Consent Searches Following the Search and Surveillance Act" (2012) 43 VUWLR 447 at 469; and Butler and Butler, above n 84, at [18.14.37].

86 McMullan, above n 85, at 462.

87 *Schreiber v Canada (Attorney-General)* [1998] 1 SCR 841 at [1].

88 At [22] and [25] per Lamer CJ and [31]–[32] per L'Heureux-Dubé J.

Lamer CJ (concurring in result) observed that the nature of the information was such that, but for the extraterritoriality of the complained actions, Mr Schreiber had a reasonable expectation of privacy in the records because they formed the "biographical core of personal information".[89]

R v Plant concerned a situation almost factually identical to *Alsford*.[90] Instead of dismissing Mr Plant's s 8 claim because the electricity consumption figures had been communicated to a third party, the Supreme Court dismissed it because the information which the police accessed was publically accessible.[91] Sopinka J argued that the communication of the information to a third party did not define reasonable expectations of privacy; instead, it was the nature of the information, of the relationship between the parties and the circumstances under which the information was obtained.[92]

In adopting those factors, Sopinka J declined to apply *Miller*, preferring La Forest J's dictum in *R v Dyment* in which his Honour (joined by Dickson CJ) stated that:[93]

> … retention of information about oneself is extremely important. We may … be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential … must be protected.

The Judge had in mind situations where a person might "wish to *maintain and control* [information] from dissemination to the state", despite the fact that the information was communicated to a third party.[94] In other words, a subject's desire to retain confidentiality in involuntarily or compulsorily disclosed information is enough for a court to conclude that a reasonable expectation of

---

89 At [22].

90 *R v Plant* [1993] 3 SCR 281 at 285.

91 At 294.

92 At 293; see also McMullan, above n 85, at 462.

93 *Plant*, above n 90, at 292, citing *R v Dyment* [1988] 2 SCR 417 at 429–430.

94 Ibid (emphasis added).

privacy is retained. *Plant*, therefore, answers the conundrum posed by the third party doctrine by circumventing the assumption of risk relied upon in *Miller*.[95] This echoes Iassacharoff and Wirshba's critique of the third party doctrine: since "knowledge of risk is [not] analytically equivalent to assumption of risk", it follows that subjects must do more to evince voluntary consent to the release of information.[96]

The Supreme Court in *R v Spencer* similarly based its inquiry on the nature of what was being searched and the impact of the search on its target.[97] The Court held that Mr Spencer had a reasonable expectation of privacy in subscriber information (name, address and telephone number – all publically accessible) obtained from his internet service provider.[98] This was because of the information's potential to link "the identified individual and the personal information provided anonymously."[99] The ISP could not consent to the release of the subscriber information because it had a "tendency … to support inferences in relation to other personal information".[100] In other words, if the police examined the subscriber details, they could link Mr Spencer to the private information regarding his criminal activity.

D The Effect of Breach of Confidence

1 Wrongdoing: maintaining a reasonable expectation of privacy

Butler and Butler argue that those who place information of wrongdoing in the hands of third parties cannot reasonably expect the police not to seek the voluntary disclosure thereof.[101] This reflects the New Zealand

---

95 See above n 67.

96 See Issacharoff and Wirshba, above n 66, at 996.

97 *R v Spencer* 2014 SCC 43 at [36].

98 At [7]–[12]; and [66].

99 At [42].

100 At [31].

101 Butler and Butler, above n 84, at 947.

courts' jurisprudence that subjects' iniquitous or criminal behaviour vitiates any argument that agencies owe them a duty of confidence.[102]

Spencer unequivocally rejected the argument that the existence of a privacy interest turns on whether it "shelters legal or illegal activity".[103] In essence, the Court adopted McLachlin J's dissent in *Plant*, in which her Honour argued that the police sought the electricity consumption information *because* it could reveal Mr Plant's wrongdoing.[104] It is arguable that, since wrongdoing will invariably (though not necessarily) be present, her Honour's position is that its presence should make no difference to the analysis. If wrongdoing were present, the mere fact of a police inquiry would be enough to validate any search after the fact.

There is a serious risk in allowing the issue of unreasonable search and seizure to be determined by what the police uncover. This reasoning (along with the rule in *Gartside* that there is no confidence in iniquity) amounts to a judicial *ex post facto* assessment. Though such an "ends-based" assessment is tempting, hindsight is capable of justifying almost any action based on the results obtained. That the police made a request does not prove that the suspect committed an illegal or iniquitous act. The Canadian and New Zealand courts have both rejected *ex post facto* assessments. Dickson J in *Hunter* noted that s 8 of the Charter is aimed at "preventing unjustified searches *before they happen*, not simply of determining, after the fact, whether they ought to have occurred in the first place".[105] Similarly, Hammond J in *Williams* stated that s

---

102 See for example, *R v H*, above n 32; and *R v Cox* and *R v Javid*, above n 34, all citing *Gartside*, above n 33.

103 *Spencer*, above n 97, at [36].

104 *Plant*, above n 90, at 302.

105 *Hunter*, above n 13, at 160 (emphasis added), cited in *Hamed*, above n 12, at [16] and [44] per Elias CJ.

21 is designed as a "prophylactic device against unjustified state intrusion *before* a search takes place."[106]

In *Tournier*, the Court of Appeal of England and Wales qualified bankers' duties of confidence with the requirement that they release information where, *inter alia*, "disclosure is under compulsion of law"; *Gartside* was not mentioned.[107] Paul Roth argues that the Privacy Act principles are a statutory "confirmation" and "endorsement" of *Tournier*.[108] It is therefore arguable that, in seeking to replicate *Tournier*'s qualifications, the Information Privacy Principles implicitly adopt "compulsion of law" as the point at which a subject's expectation of privacy must give way to the public interest. This would have the function of preventing police from relying on *Gartside* to since agencies would be incapable of consenting in the absence of a production order.

2 Enforcing duties of confidence against police

The release of information by an agency in breach of confidence vitiates the agency's consent per *Sanders*. Even in the absence of an agency's breach of confidence, it may be possible to hold the police liable for the use of that information. In *Hunt v A*, Ms Hunt wrote a book which included W's claims that a medical professional, A, had sexually assaulted her, along with information regarding the subsequent confidential settlement.[109] A brought a claim against Ms Hunt for breach of confidence on the basis that W owed A a

---

106 *Williams*, above n 60, at [263] (emphasis added), commenting on *Entick v Carrington* (1765) 19 Howell's State Trials 1029, 95 ER 807.

107 *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461 (CA) at 473 per Bankes LJ.

108 Paul Roth *Privacy Law and Practice* (online looseleaf ed, Lexis Nexis, updated to April 2016) at [BNF.2] and [BNF.2(a)]; see for example principles 10 and 11, Privacy Act 1993, s 6.

109 *Hunt v A*, above n 30, at [5], [8], [9] and [26].

duty of confidence and that Ms Hunt therefore improperly used the information she had consensually obtained from W.[110]

Regarding outsiders to a duty of confidence, the Court held that liability would lie against an "acquirer" who "acted unconscionably in relation to the acquisition [or use] of the information".[111] Unconscionability is determined by:[112]

(1) the nature of the information; and

(2) any liability on the part of the "acquirer and discloser" for any breach of confidence.

Moreover, if the acquirer had actual knowledge that a duty of confidence existed, they would be presumed to have acted unconscionably and face "almost insuperable difficulties" in displacing that presumption.[113]

Application of *Hunt* to WRCIs is factually difficult. It is hard to ascertain whether police are aware that agencies hold information subject to duties of confidence (if the agency in fact does). Certainly, in relying on IPP11(e)(i), officers must be aware that agencies have a duty not to release information unless the exception applies; but this is not equivalent actual knowledge of a duty of confidence. It is thus hard to conclude in the abstract whether or not a duty of confidence between a subject and an agency will bind the police.

---

110 At [66] and [67].

111 At [92].

112 At [93].

113 At [94].

IV Are WRCIs Unreasonable?

The current approach as to whether a search or seizure is unreasonable is set out in *Hamed*. A search may be unreasonable "because it occurred at all or because of the unreasonable manner in which it was carried out."[114] Putting aside the latter, an unlawful search is normally an unreasonable one,[115] unless the "breach [was] minor or technical", if the police reasonably believed their actions were lawful,[116] or if they could discharge a "significant persuasive burden" to show that the search was not unreasonable.[117]

This Part argues that WRCIs are not authorised by law and are thus prima facie unreasonable. In particular, this Part argues that the production order regime has excluded any common law right that the police might have to conduct WRCIs. Moreover, it is arguable that the policy issues surrounding WRCIs mean that courts should hold them to amount to an unreasonable search or seizure per s 21.

Since this paper argues that WRCIs are unlawful per se, it is unnecessary (and impossible in the abstract) to examine whether they might become unreasonable because of the manner in which they are carried out.

A Are WRCIs lawful?

Lawfulness is a question of whether the search or seizure should have "occurred at all".[118] We are concerned with the request, rather than the receipt. The first question is whether any statute authorises WRCIs. If there is, that is the end of the inquiry. If not, WRCIs are prima facie unreasonable. A further consideration is that, despite not being authorised by statute, WRCIs may

---

114 *Hamed*, above n 12, at [172] per Blanchard J.

115 At [174] per Blanchard J and at [226] per Tipping J.

116 At [174] per Blanchard J.

117 At [226] per Tipping J.

118 At [172] per Blanchard J.

nonetheless be authorised by a "third source of power", which allows police to conduct WRCIs in the absence of any law expressly prohibiting them.[119]

It must be noted that this Part deals with police requests under ordinary circumstances, ignoring requests made in exigent circumstances – such as missing persons, abductions or other life-threatening cases, in which time is of the essence. In such cases, the time required to obtain a production order (which this paper argues should be the legal requirement for police requests) would likely have an intolerable impact on the outcome.[120] Indeed, there is ample authority that the code created by the SSA does not cover exigent circumstances.[121] Similarly, where a warrant could have been sought, a warrantless search will be unreasonable absent necessity.[122]

1 The Privacy Act 1993

One could argue that principle 2 authorises police requests. It requires that agencies "shall collect … information directly from the individual concerned" unless doing so would cause "prejudice to the maintenance of the law". Per that argument, police may obtain information from agencies if collecting it from the subject would prejudice the maintenance of the law. However, principle 2 is one of the "Information Privacy *Principles*"[123] – a principle does not amount to an authorisation and nothing therein confers a power to collect information. In essence, principle 2 states that *if* a power to collect information is exercised, it *must* be exercised in accordance with principle 2.

---

119 See *Hamed*, above n 12, at [217] per Tipping J; see also *Ngan*, above n 52, at [46] per Tipping J and at [100] per McGrath J.

120 Law Commission R97, above 85, at [5.4].

121 See for example *Ashby v R* [2013] NZCA 631, [2014] 2 NZLR 453 at [50]; and Search and Surveillance Act 2012, s 14.

122 Law Commission R97, above n 85, at [5.65]; *R v Laugalis* (1993) 10 CRNZ 350 (CA) at 356; see also *Williams*, above n 60, at [24].

123 Emphasis added.

Principle 11, upon which the police most explicitly rely when making WRCIs,[124] is couched in similar terms: agencies must not disclose information unless they believe on reasonable grounds that non-compliance is necessary to avoid prejudice to the maintenance of the law. This exception immunises agencies which disclose personal information, protecting them from liability under the Privacy Act if the Privacy Commissioner determines that the release was warranted by IPP11(e)(i) – it is a shield for agencies.

Privacy Act relationships are between subjects and agencies; nothing implicates the police or implies that principle 11 is a sword for police. An agency's power to disclose does not correlate with a police right to seek that information; nor does the Privacy Act confer a right upon the latter to seek disclosure, which would place any duty upon the agency to accede to WRCIs.[125] Additionally, the police practice of seeking a warrant in the event of refusal militates against a conclusion that police have a power which disables an agency from resisting disclosure – if the police had the power to compel disclosure, a warrant would be unnecessary.[126]

The Law Commission has attempted to clarify the position regarding principle 11. In their review of the Privacy Act, the Commission stopped short of recommending that the principle be interpreted or amended to authorise WRCIs, recommending instead that the principle be redrafted to specifically cover agencies' ability to disclose information about offending.[127] The Commission also recommended that the Privacy Commissioner formulate

---

124 See for example *Hager* Key Evidence Bundle Volume 4, above n 8 at PD 4/562 and PD 4/650-651.

125 But see *Harris*, above n 27, in which there was a statutory duty upon the bank to report.

126 See for example *Thompson* (1995), above n 27, at 549; and *Cox*, above n 27, at [11].

127 Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011) at [9.49]; for a comparison with the common law position, see *R v Harris*, above n 27.

guidance on how to respond to police requests.[128] Although the Law Commission's clarifications might imply a police power to request information, the report did not distinguish between ordinary requests and those in exigent circumstances.[129] As such, it is difficult to ascertain whether the Commission was referring to actions that are already held to be lawful or whether they were referring to WRCIs in general.

2 The Policing Act 2008

Finally, the Policing Act 2008 could confer upon police the power to make requests. Section 9 states that the Police's functions are, *inter alia*, to enforce the law and to prevent crime.[130] The Act need not specify that WRCIs are permissible, as common law permits those exercising statutory powers to "do other things fairly incidental to express purposes" without "circumvent[ing] or undermine[ing] the proper statutory purpose".[131] WRCIs could be seen as an incidence of these statutory functions.

However, that section must be read in the context of s 8, which declares that the Act is based the principle that policing services "are a cornerstone of a *free and democratic society under the rule of law*" and "are provided in a manner that *respects human rights*."[132] Therefore, arguing that s 9 empowers police to make WRCIs begs the question. Since the powers contained in s 9 must be read subject to the principles contained in s 8 (which might be read as

---

128 At [9.46]; some cursory guidance can be found at the following address: <www.privacy.org.nz/further-resources/knowledge-base/view/225?t=5453_7465> (accessed 26 August 2016).

129 See above at n 121.

130 Paragraphs (c) and (d).

131 *Attorney-General v Ireland* [2002] 2 NZLR 220 (CA) at [39]–[40]; and *New Zealand Airline Pilots' Association Industrial Union of Workers Incorporated v Civil Aviation Authority of New Zealand* HC Wellington CIV-2011-485-954, 13 July 2011 at [74], citing *Ashbury Railway Carriage & Iron Co Ltd v Riche* (1875) LR 7 HL 653 (HL) and *Attorney-General v Great Eastern Railway Co* (1880) 5 App Cas 473 (HL).

132 Paragraphs (a) and (d) (emphasis added).

subjecting s 9 to NZBORA), s 9's interpretation turns on the conclusion of this paper. Since this paper argues that WRCIs breach s 21, s 9 cannot provide arguments either way, except perhaps regarding exigent circumstances.

3 The "third source of power" for state authority

Having concluded that no positive law authorises WRCIs, the question is now whether WRCIs are a residual power of police under the "third source doctrine". Regarding police powers, Bruce Harris makes three points about the third source. First, it is unable to "override legal rights";[133] secondly, its use can only be justified by the "pragmatic need for the police to be able to take legitimate action to address the unexpected";[134] and thirdly, it now plays a much less significant role in policing due to the "extensive authority deliberately given to the police by statute".[135] On this basis, the claim that WRCIs fall within the third source doctrine fails on the second point as such requests are aimed at routine police needs, rather than unexpected occurrences.

Ignoring this matter for the moment, let us assume, for the purposes of Harris's first point, that no privacy interests are implicated. Even then, we might doubt that third source powers authorise WRCIs. The *Quake Outcasts* case looked at whether a statute "covered the field", thus excluding recourse to the third source doctrine.[136] A majority of the Supreme Court found that the Canterbury Earthquake Recovery Act 2011 covered the field: relevantly because the Act's purposes were "expressed comprehensively", demonstrating that the Act was "the only vehicle" for the exercise of power;[137] and because the Act aimed to safeguard against oppressive behaviour by requiring that any

---

133 BV Harris "Recent Judicial Recognition of the Third Source of Authority for Government Action" (2014) 26 NZULR 60 at 61.

134 At 62.

135 At 70.

136 *Quake Outcasts v Minister for Canterbury Earthquake Recovery* [2015] NZSC 27, [2016] 1 NZLR 1 [*Quake Outcasts*].

137 At [115].

power exercised under the Act must be used solely for the purposes stated therein.[138] Quoting Lord Atkinson in *De Keyser's Royal Hotel Ltd*, Glazebrook J noted that it would be "useless and meaningless for the Legislature to impose restrictions and limitations" on Crown powers "if the Crown were free at its pleasure to disregard these provisions."[139] This echoes Harris's third point.

Thus, the question is whether Parliament has imposed limitations on police exercise of power such that it is unlawful for police, absent exigent circumstances, to make WRCIs. Under s 72 of the SSA production orders can be issued only if the applicant has reasonable grounds to:

(1) "suspect that an offence has been committed"; and
(2) "believe that the documents sought … constitute [relevant] evidential material" and are in the possession of the person to whom the order is directed.

This is nearly identical to the requirement under IPP11(e)(i) that agencies must not release personal information unless they have reasonable grounds to believe that withholding the information would cause "prejudice to the maintenance of the law". Implicit in IPP11(e)(i) is that the agency must satisfy itself that an offence has actually been committed. Though "prejudice to the maintenance of the law" is left undefined, it is arguable that the police's inability to advance a criminal investigation would fall within this definition. If police must demonstrate the same factors to obtain production orders as agencies must have to release information, production orders would clearly demonstrate to agencies that IPP(11)(e)(i)'s requirements were satisfied. Given, therefore, that the two regimes cover the same situations in the same (or nearly the same) manner, it is arguable that the SSA covers the field and excludes the jurisprudence on WRCIs.

---

138 At [118].

139 At [111], citing *Attorney-General v De Keyser's Royal Hotel Ltd* [1920] AC 508 (HL) at 539.

It is also important that the powers conferred by the SSA are to be exercised in a "manner that is consistent with human rights", namely the rights contained in NZBORA, the Privacy Act and the Evidence Act.[140] This explicit conferral of powers, combined with the affirmation of express safeguards arguably makes the Act a code, covering the field and excluding the previous common law or third source justifications for WRCIs.[141]

B Policy Concerns Regarding WRCIs

Having found that WRCIs are unlawful, *Hamed* indicates they are presumptively unreasonable unless the police can show, on the facts, that the court should hold the action reasonable.[142] Since this is a largely case-specific inquiry, this paper will not examine this point. However, there are some further policy arguments demonstrating that WRCIs are unreasonable.

New Zealand's courts have treated agencies as if they were police informants: like any other civically-minded citizen, agencies should be allowed to provide information concerning wrongdoing to police.[143] Encouraging agencies to report suspected crimes is in the public interest and to prohibit this would impede the police's ability to investigate crime. But a distinction must be drawn between this (along with witness disclosures to police) and WRCIs. To obtain disclosure, the former relies on the discloser's initiative whilst the latter relies on a request carrying the weight of police necessity which risks engendering a sense of apparent compulsion in recipients.

Our courts' lack of distinction ignores the practical realities of our modern information society, diminishing the scope of protection for personal

---

140 Search and Surveillance Act 2012, s 5.

141 See Bruce Robertson (ed) *Adams on Criminal Law* (online looseleaf ed, Brookers, updated to 9 Jult 2016) at [SSIntro.02] and [SS3.43.01]; and *Ashby*, above n 121, at [48].

142 *Hamed*, above n 12, at [174].

143 See for example *R v H* and *R v Harris*, above n 27.

information. Agencies may compulsorily gather and hold information for many years, during which time the state can conscript it against individuals. This risks allowing state access to almost every piece of information we generate in our lives, enabling a dedicated investigator to build up a detailed (though not necessarily accurate) picture of our lives. Furthermore, the more time elapses between the information's creation and its conscription by the state, the harder it becomes for the subject to recall how the information came into being and thus harder to challenge its accuracy. In an age where so many different entities hold personal information, the New Zealand approach makes s 21 virtually redundant except regarding physical searches. After all, if the state can make WRCIs without consequence, what sphere of informational privacy is left to s 21?

Furthermore, under the New Zealand courts' interpretation, police can, without assessing the legal implications, seek disclosure of information which if granted, could be taken as evidence of the lawfulness thereof. Moreover, it is unrealistic to expect all agencies to have the resources to conduct an IPP11(e)(i) analysis, especially when police assert the necessity of disclosure without providing any substantial level of detail as to why the information is required.[144] Concerns at the use of warrantless powers are reflected in a three month investigation undertaken by the Privacy Commission. That report revealed that the 10 corporate bodies participating received 11,799 requests, of which all but three per cent were accepted.[145] Furthermore, participants recorded that 1,014 requests were made under the Privacy Act, reflecting an erroneous belief that the Act provides government agencies with the power to compel disclosure.[146] Given the apparent formality of request documents, there is a real risk that an agency, particularly one

---

144 See for example *Hager* Key Evidence Bundle Volume 4, above n 8, at PD 4/558–565.

145 Office of the Privacy Commissioner "Transparency Reporting Trial", above n 21, at [25] and [49].

146 At [39].

unfamiliar with these procedures, will perceive that they are legally obliged to accede.[147]

A further issue is that the lack of judicial oversight renders WRCIs vulnerable to falling afoul of evidential protections such as journalistic privilege. In *Hager*, the police were held to have failed to discharge their duty of candour because they failed to raise the issue of journalistic privilege.[148] By allowing WRCIs, courts risk seriously undermining the protections provided by both the common law and the SSA.[149]

The argument against the approach this paper espouses is that such a stance on WRCIs would chill police investigations in their initial stages, rendering some vulnerable to being abandoned for lack of evidence. It would thus present an intolerable impediment to police investigations and to the maintenance of the law: suspects might be adept at hiding evidence of their crimes, or be able to destroy evidence before police can obtain it. But first, as Issacharoff and Wirshba prosaically put it: "there is little risk that data or documents held by third parties will drive off into the sunset … as with vehicles".[150] Secondly, it would not unduly hamper police investigations because, though the advocated approach removes an investigative technique, many others remain. In any case, no state agent should be allowed to use unlawful techniques to obtain information, even if reliance on lawful methods would prove much more onerous. If a shortcut is unlawful, it should not be used and the courts should not countenance its use contrary to s 21's fundamental principles. To hold, as New Zealand's courts have, that WRCIs implicate no privacy interests dangerously undermines the protection afforded by s 21 in the digital era, based on *ex post facto* assessments of iniquity.

---

147 See [43]–[44]; see *Hager* Key Evidence Bundle Volume 4, above n 8, at PD 4/558–565 as an example of police reliance on principle 11.

148 *Hager*, above n 2, at [121].

149 See Search and Surveillance Act 2012, s 136.

150 Issacharoff and Wirshba, above n 66, at 1019.

Section 21 cannot abide by means of investigation that are justified by the ends achieved.

V Conclusion

The New Zealand courts' approach to WRCIs does not reflect the first principles approach to s 21 espoused by the Canadian cases or by *Hamed*. Importantly, the approach is also no longer suited to the digital age. This paper has argued that our courts must reformulate their approach to better reflect these fundamental principles. Particularly, it should not be permissible for courts to dismiss claims by reliance on *ex post facto* findings of complainants' iniquitous or criminal behaviour as such an approach is not consistent with the disavowal of *ex post facto* justification espoused in *Williams* and *Hunter*.

This paper has also argued that, notwithstanding the likely inconvenience to police, WRCIs are neither lawful nor reasonable. In any case, following the enactment of the SSA, the police have ample tools to compel agencies to disclose information. It follows that, except in urgent cases, agencies should not disclose information to police except upon receipt of a production order. To do otherwise would make banks, power companies and the like complicit in the erosion of reasonable expectations of privacy and would fly in the face of agencies' obligations of confidence.

If this means that the police must let (suspected) cannabis cultivators or methamphetamine dealers go free for want of evidence, so be it; it is worth it to preserve the freedom of citizens (including journalists, activists and the like) to be free from having their "secret affairs" intruded upon, "read over" and "pried into".[151]

---

[151] To use the words of the plaintiff's plea in *Entick*, above n 106, at 1029.

VI Bibliography

A Cases

1 New Zealand

Ashby v R [2013] NZCA 631, [2014] 2 NZLR 453.

Attorney-General v Ireland [2002] 2 NZLR 220 (CA)

Hager v Attorney-General [2015] NZHC 3268, [2016] 2 NZLR 523.

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

Hunt v A [2007] NZCA 332, [2008] 1 NZLR 368.

Lorigan v R [2012] NZCA 264, (2012) 25 CRNZ 729.

New Zealand Airline Pilots' Association Industrial Union of Workers Incorporated v Civil Aviation Authority of New Zealand HC Wellington CIV-2011-485-954, 13 July 2011.

Quake Outcasts v Minister for Canterbury Earthquake Recovery [2015] NZSC 27, [2016] 1 NZLR 1.

R v Alsford [2015] NZCA 628.

R v Cox (2004) 21 CRNZ 1 (CA).

R v H [1994] 2 NZLR 143 (CA).

R v Harris [2000] 2 NZLR 524 (CA).

R v Javid [2007] NZCA 232.

R v Jefferies [1994] 1 NZLR 290 (CA).

R v Ngan [2007] NZSC 105, [2008] 2 NZLR 48.

R v Sanders [1994] 3 NZLR 450, (1994) 12 CRNZ 12 (CA).

R v Thompson (1995) 13 CRNZ 546 (HC).

R v Thompson [2001] 1 NZLR 129 (CA).

R v Williams [2007] NZCA 52, [2007] 3 NZLR 207.

S v Police (2002) 22 FRNZ 28 (HC).

2 England and Wales

Entick v Carrington (1765) 19 Howell's State Trials 1029, 95 ER 807.

Tournier v National Provincial and Union Bank of Enland [1924] 1 KB 461 (CA).

3 Canada

Hunter v Southam Inc [1984] 2 SCR 145.

R v Cole [2012] SCC 53, [2012] 3 SCR 43.

R v Plant [1993] 3 SCR 281.

R v Spencer [2014] SCC 43.

R v Wise [1992] 1 SCR 527.

Schreiber v Canada (Attorney-General) [1998] 1 SCR 841.

4 United States

Katz v United States 389 US 347 (1967).

United States v Jones 132 S Ct 945 (2012).

United States v Miller 425 US 435 (1976).

B Legislation

1 New Zealand

New Zealand Bill of Rights Act 1990.

Policing Act 2008.

Privacy Act 1993.

Search and Surveillance Act 2012.

2 Canada

Canadian Charter of Rights and Freedoms.

C Books and Chapters in Books

Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis, Wellington, 2015).

D Journal Articles

Samuel Beswick "Perlustration in the Pathless Woods: *Hamed v R*" (2011) 17 Auckland U L Rev 291.

Harriet Bush "The Video Camera Surveillance (Temporary Measures) Act 2011: An Unprecedented Licence to Search?" (2013) 44 VUWLR 221.

Christopher Harker "Consent Searches and Section 21 of the New Zealand Bill of Rights Act 1990" (2011) 9 NZJPIL 137.

BV Harris "Recent Judicial Recognition of the Third Source of Authority for Government Action" (2014) 26 NZULR 60.

Lucas Issacharoff and Kyle Wirshba "Restoring Reason to the Third Party Doctrine" (2016) 100 Minn L Rev 987.

Sam McMullan "Third Party Consent Searches Following the Search and Surveillance Act" (2012) 43 VUWLR 447.

Scott Optican "What is a "Search" under s 21 of the New Zealand Bill of Rights Act 1990? An Analysis, Critique and Tripartite Approach" [2001] NZ L Rev 239.

E Legal Encyclopaedias and Looseleaf Texts

Laws of New Zealand (online ed).

Dictionary of New Zealand Law (online ed, LexisNexis).

Bruce Robertson (ed) *Adams on Criminal Law* (online looseleaf ed, Brookers, updated to 9 July 2016).

Paul Roth *Privacy Law and Practice* (online looseleaf ed, Lexis Nexis, updated to April 2016).

F New Zealand Law Commission Reports

Law Commission *Search and Surveillance Powers* (NZLC R97, 2007).

Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011).

G Legal Submissions, Evidence Bundles and Affidavits

Hager v Attorney-General Key Evidence Bundle Volume 1: Applicant's Affidavits CIV 2014-485-11344.

Hager v Attorney-General Key Evidence Bundle Volume 4: Key Police Disclosures CIV 2014-485-11344.

Hager v Attorney-General CIV 2014-485-11344 Written Submissions for the Applicant CIV 2014-485-11344.

H Other Sources

Office of the Privacy Commissioner "Transparency Reporting Trial Aug–Oct Full Report" (18 February 2016) Privacy Commissioner <www.privacy.org.nz>.

Word count

The text of this paper (excluding table of contents, footnotes, abstract and bibliography) is exactly 7,995 words.