Chapter 2 – The scope of the Act

INTRODUCTION

2.1 The current scheme of the Search and Surveillance Act 2012 (the Act) is very specific about the type of law enforcement conduct that may be authorised where surveillance is concerned, but takes a permissive approach to the issuing of search warrants. This chapter considers some potential problems that have arisen as a result of that approach. We ask whether it is desirable—and even possible—to clarify the type of conduct that amounts to a "search" or "surveillance" and should fall within the scope of the Act.

2.2 The search warrant regime in the Act enables warrants to be issued where certain criteria are met but does not specify when a warrant must be obtained. The surveillance device warrant regime *does* require a warrant to be obtained before certain types of surveillance are carried out, but it only provides for warrants in relation to a limited subset of what might be considered "surveillance".

2.3 While this may not have been of significance at the time the Act was drafted, our discussions with enforcement agencies suggest that—with the emergence of new technologies—it is beginning to cause difficulties. There is uncertainty about the extent to which investigatory methods that were not anticipated by the Act can be used. In practical terms, this means enforcement agencies are sometimes unable to use the best tool for a job due to uncertainty about its lawfulness (even though, as we discuss further in Chapter 3, these new tools are sometimes no more intrusive than methods that the Act currently permits).

2.4 In this chapter we outline the scope of the authorisation regime in the Act, identify where there are gaps, and suggest some possible alternatives to the current approach. Among the options we discuss are:

- defining at a high level what class of conduct impacts on an individual's rights in such a manner that a warrant (or other form of authorisation) should be required; and
- including a residual warrant regime in the Act, which would permit (or potentially require) enforcement agencies to obtain a warrant to carry out types of activity that are not captured by the search or surveillance device warrant regimes in the Act.

2.5 Subsequent chapters consider how specific investigatory techniques should be regulated in more detail.

THE CURRENT LAW

What is a search?

2.6 Under the Act, issuing officers may issue a search warrant in relation to a place, vehicle or thing on application by a constable if satisfied there are reasonable grounds:[1]

- to suspect that an offence specified in the application and punishable by imprisonment has been, is being or will be committed; and
- to believe that the search will find evidential material in respect of the offence in or on the place, vehicle or thing.

2.7 "Search" is not defined in the Act. However, it is clear that a search warrant permits the person executing it to enter and search the place, vehicle or thing specified, and any items found there.[2] The searcher may also seize or copy anything that is the subject of the search (as specified in the warrant) or that is in "plain view".[3]

2.8 Searches can be anticipatory—they may be issued in relation to an offence that "will be committed"[4]—but they cannot allow continuous surveillance or monitoring. A search is treated as a discrete event. So, although a warrant can permit searches on multiple occasions, each warrant must specify the number of times it can be exercised.[5] A search warrant is generally valid for a maximum of 14 days from the date of issue.[6] Ongoing surveillance is authorised under the surveillance device warrant regime, which is discussed below.[7]

---

1 Search and Surveillance Act 2012, s 6.

2 Section 110(a).

3 Sections 110(d), 110(g) and 123. The plain view seizure power only applies where the enforcement officer has reasonable grounds to believe that a search warrant could have been obtained or that a search power could have been exercised that would allow seizure of the item.

4 Section 6(a).

5 Section 103(j).

6 Section 103(h).

7 See paragraph [2.19] of this Issues Paper onward.

2.9 There is nothing in the Act that requires New Zealand Police to obtain a search warrant in particular circumstances. Rather, it is left to constables to determine on a case-by-case basis when it is necessary or appropriate to seek a warrant. Often, the intended course of action would or may be unlawful in the absence of a warrant. For example, searches of private property will generally constitute trespass if no warrant is obtained.

2.10 If evidence is obtained as a consequence of an unlawful or unreasonable search, it may constitute a breach of section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA). Further, the evidence may be excluded from criminal proceedings under section 30 of the Evidence Act 2006 (although whether this will happen depends on the exercise of judicial discretion). This provides a clear incentive for enforcement agencies to seek a warrant if they are in doubt as to whether the intended course of action is lawful or not – assuming a warrant is available. Our impression from speaking to enforcement agencies was that they generally take a cautious approach. However, this is a matter of internal policy and the practice of individuals rather than a specific legislative requirement.

Reasonable expectations of privacy

2.11 Unfortunately, determining whether conduct by enforcement officers is lawful or unlawful is not always a straightforward exercise.

2.12 In determining whether something is a "search" so as to engage section 21 of NZBORA, the New Zealand courts have generally adopted a similar test as is applied in the United States and Canada.[8] This involves asking whether the activity amounts to a State intrusion on reasonable expectations of privacy.[9] An expectation of privacy will only be reasonable if:[10]

---

8 *R v Wise* [1992] 1 SCR 527 at 533; *Hunter v Southam Inc* [1984] 2 SCR 145 at 159; *Katz v United States* 389 US 347 (1967) at 360–361.

9 The test for what amounts to a search was discussed at length by the Supreme Court in *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305. While no clear ratio emerges from that decision, the Court of Appeal has subsequently taken the approach that the test of "state intrusion into reasonable expectations of privacy" is broadly consistent with the *Hamed* judgments and should be applied: *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22]. See also *Maihi v R* [2015] NZCA 438 at [20].

10 *Hamed v R*, above n 9, at [163] per Blanchard J.

> … first, the person complaining of the breach of s 21 did subjectively have such an expectation at the time of the police activity and, secondly, that expectation was one that society is prepared to recognise as reasonable.

2.13 Once it has been established that there was a "search", the reasonable expectations of privacy test is also relevant in assessing whether the search was, in terms of section 21 of NZBORA, unreasonable.[11]

2.14 The concept of a reasonable expectation of privacy is considerably broader than the traditional understanding of a "search" at common law, which generally required a trespassory interference with a person's property rights.[12] Conduct that amounts to an intrusion on reasonable expectations of privacy may include, for example, video surveillance of a public area using night-filming capabilities[13] even if no trespass is involved.

2.15 The courts have not always found the concept easy to apply. This is shown by courts in the United States and Canada—despite applying the same test—reaching different conclusions about whether similar types of activity constitute a "search".[14] In New Zealand, courts have on occasion declined to decide whether something is a search at all and have instead assessed whether the conduct in question is "reasonable".[15] Enforcement agencies told us it is not always clear to them when a warrant is needed.

2.16 The reasonable expectation of privacy test has been criticised on the basis that it is uncertain (leading to inconsistent results), circular and unable to adapt adequately to the digital environment.[16]

---

11 *Hamed v R*, above n 9, at [163] per Blanchard J.

12 See for example *Entick v Carrington* (1765) 19 St Tr 1030, 2 Wils KB 275.

13 *Lorigan v R*, above n 9, at [25].

14 See *Kyllo v United States* (2001) 533 US 27 and *R v Tessling* [2004] 3 SCR 432 (thermal imaging devices); *United States v Place* 462 US 696 (1983), *R v AM* [2008] 1 SCR 569 and *R v Kang-Brown* [2008] 1 SCR 456 (drug detection dogs); *Lopez v United States* 373 US 427 (1963) and *R v Duarte* [1990] 1 SCR 30 (participant recordings of private conversations).

15 For example *Maihi v R*, above n 9, at [17]–[29]. See also the discussion in *Tararo v R* [2010] NZCA 287, [2012] 1 NZLR 145 at [51]–[64] (relating to the position pre-*Hamed*) and the Supreme Court's decision in *Tararo v R* [2010] NZSC 157, [2012] 1 NZLR 145 at [7].

16 See for example Renée McDonald Hutchins "The Anatomy of a Search: Intrusiveness and the Fourth Amendment" (2010) 44 U Rich L Rev 1186; Brandon Crowther "(Un)Reasonable Expectation of Digital Privacy" (2012) BYU L Rev 343; Micah Peterson "The Shrinking Window of Privacy: The Decision in *Skinner* and How it Opens Wider the Prying Eyes of Government" (2013) 49 Tulsa L Rev 183; *Kyllo v United States*, above n 14, at 34; and Olga Ostrovsky "Search Under

2.17 The circular element of the test stems from the fact that an individual's expectation of privacy, and whether society considers that to be reasonable, is influenced by State actions. If a State intrusion on privacy becomes more prevalent and publicly apparent, people are less likely to have a subjective expectation that their activities will remain private. Even where they do, the courts may be less willing to find that their expectation is one that society would consider reasonable. After all, if we know that surveillance is widespread, can we still reasonably expect not to be subjected to it?

2.18 The argument that the test does not work well in a digital setting is advanced on a number of grounds. Among these are:[17]

- Judges base their assessment of what is "reasonable" on the nature of the underlying technology, but this may not accord with the public's understanding. As digital technology develops, there may be an increasing gap between what a judge is willing to recognise as private and what an individual subjectively expects to be private. For example, people's activity on the Internet may "produce a much larger data trail than most people expect, and portions of that data trail are available to more people and companies than most would expect".[18]
- Data is often disclosed for the limited purpose of accessing a service. For example, it is usually a condition of using an online service that the provider can keep a record of the user's activity and draw on that data for advertising or other specific purposes. Agreeing to such a condition may mean that a person no longer expects the information to be private in a general sense; however, it does not necessarily mean that he or she would expect it to be available to the State for law enforcement purposes.
- It may be relatively easy for a judge to assess what society views as a reasonable expectation of privacy in the context of a physical search or the covert recording of a conversation. However, such an assessment becomes difficult when dealing with complex technology, not least because there may not be a consistent societal

---

Surveillance: The Meaning of "Search" under Section 21 of the New Zealand Bill of Rights Act 1990" (LLB (Hons) Dissertation, University of Auckland, 2012).

17 See the discussion in Crowther "(Un)Reasonable Expectation of Digital Privacy", above n 16, at 351–363.

18 Crowther "(Un)reasonable Expectation of Digital Privacy", above n 16, at 351.

view of what is reasonable in that context. For example, people of different ages or with different levels of technological expertise may have very different expectations of privacy in respect of information generated by their Internet use.

What is surveillance?

2.19 The surveillance regime in the Act governs the use of "surveillance devices", which are exhaustively defined as an interception device, tracking device or visual surveillance device.[19]

2.20 "Surveillance" is not itself defined in the Act. In this Issues Paper we use the term to refer to the observation or monitoring of people, places, things, data or communications. In comparison to a search, which is a discrete event, surveillance can be continuous over a prolonged period. Under the Act, a single warrant can authorise surveillance for up to 60 days.[20]

2.21 While the Act differentiates between searches and surveillance activity for authorisation purposes, they are treated the same in terms of section 21 of NZBORA. The reasonable expectation of privacy test for determining whether activity is a search under section 21 may equally capture conduct that might be classed as surveillance. This means that, as with searches, the reasonableness of surveillance activity may be challenged in proceedings under section 21 and any associated evidence may be excluded under section 30 of the Evidence Act.

2.22 Unlike the search warrant regime discussed above, the Act *requires* enforcement officers to obtain a surveillance device warrant before conducting certain types of surveillance. These are:[21]

- the use of an interception device to intercept a private communication (unless authorised under the Act, this is an offence under the Crimes Act 1961[22]);
- the use of a tracking device;[23]

---

19 Search and Surveillance Act 2012, s 3 (definition of "surveillance device").

20 Section 55(1)(c). In comparison, a search warrant is generally only valid for up to 14 days from the date of issue: see s 103(h).

21 Section 46.

22 Crimes Act 1961, s 216B.

23 A warrant is required except where the device is installed solely for the purpose of ascertaining whether a thing has been opened, tampered with, or in some other way dealt with, and where the installation of the device does not involve trespass to land or trespass to goods: see s 46(1)(b) of the Search and Surveillance Act 2012.

- the use of a surveillance device that involves trespass to land or goods; and
- the use of a visual surveillance device to observe and/or record private activity[24] in private premises, or to observe and/or record private activity in the curtilage[25] of private premises if the observation lasts for a certain duration.[26]

2.23 In addition to the requirement to obtain a warrant, any surveillance involving trespass and any use of interception devices may only be carried out in relation to offences punishable by at least seven years' imprisonment, or certain other specified offences.[27] This applies to *any surveillance* involving trespass, even though the Act does not define "surveillance" and only provides for warrants in relation to the use of surveillance *devices*.

2.24 As will be apparent, the surveillance device warrant regime is not a comprehensive authorisation regime for surveillance activities. Surveillance that does not use a device (such as following a person in a car or peering over a fence) or that uses devices other than those listed in the Act is not captured. This may limit the ability of the Act to deal with emerging technologies. For example, there is now laser technology that can screen people or luggage for chemical residue (such as drugs or explosives). This would not appear to be covered by the surveillance device warrant regime.[28]

2.25 Further, the use of an interception device is only captured by the regime if it involves intercepting a "private communication". This is because it was intended to offset section 216B of the Crimes Act 1961, which makes it an offence to intercept a private communication using an interception device (in the absence of authorisation). The

---

24 "Private activity" is defined in s 3 of the Search and Surveillance Act 2012 as activity that any one or more of the participants ought reasonably to expect is being observed or recorded by no one except the participants.

25 The term "curtilage" is not defined in the Search and Surveillance Act 2012 and bears its ordinary meaning (encompassing the land immediately surrounding a house or building, including any closely associated buildings and structures, but excluding any associated open fields beyond them: see Simon France (ed) *Adams on Criminal Law – Rights and Powers* (online looseleaf ed, Thomson Reuters) at [SS46.08(2)]).

26 That duration is three hours in any 24-hour period or eight hours in total for the purposes of a single investigation or a connected series of investigations: see s 46(1)(e) of the Search and Surveillance Act 2012.

27 Search and Surveillance Act 2012, ss 45 and 3 (definition of "trespass surveillance"). The specified offences are under the Arms Act 1983 and Psychoactive Substances Act 2013.

28 We note that in some circumstances such a device could be used as part of a "search", as "equipment" can be used by a person exercising a search power (s 110(e)). However, as we have noted, searches are treated as discrete events, so search powers would not allow ongoing monitoring over an extended period of time (for example, setting up a drug residue detector outside the premises of a suspected drug dealer to identify whether people leaving the premises are in possession of illegal substances).

definition of "private communication" raises a number of issues that will be discussed in Chapter 4. At this stage, we simply note that the definition is fairly limited in scope. For example, the definition assumes there must be two or more people involved in a communication, so it would not appear to capture machine-to-machine communications or "metadata".[29]

2.26 The Act does not specifically require enforcement officers to obtain authorisation before carrying out surveillance not covered by the surveillance device warrant regime. Nor does it provide for enforcement officers to obtain a warrant in such cases. In practice, if enforcement officers wish to undertake investigatory surveillance activity not covered by the Act, a case-by-case assessment must be made of whether the proposed activity is likely to invade a person's reasonable expectation of privacy.

Declaratory orders

2.27 The complexity of the "reasonable expectation of privacy" test and the limited scope of the surveillance device warrant regime create some ambiguity about when and how novel investigatory methods can be used.

2.28 The Act does anticipate this and contains a mechanism for enforcement officers to receive in advance some level of assurance that the use of novel devices or techniques is lawful. An enforcement officer can apply for a "declaratory order" if he or she wishes to use a device or technique that is not specifically authorised in legislation and "may constitute an intrusion into the reasonable expectation of privacy of any other person".[30]

2.29 A declaratory order is a statement by a judge that he or she is satisfied the proposed course of action is reasonable and lawful.[31] The order is advisory in character and does not bind subsequent courts.[32]

---

29 Search and Surveillance Act 2012, s 3 (definition of "private communication"). Metadata includes information associated with a communication, such as the time and date of an email or text message, the location or IP address it was sent from, who it was sent by and who the intended recipient was.

30 Section 66.

31 Section 65(1).

32 Section 65(2).

The legislative history of declaratory orders

2.30 At the time the Search and Surveillance Bill was drafted, it appears the intention was to *require* a warrant, subject to express exceptions, for any law enforcement action that might invade a reasonable expectation of privacy. The introduction version of the Bill included a "residual warrant" regime, which would have required authorisation by warrant for intrusive actions not covered by other provisions. Clause 57 of the Bill provided:[33]

> **57 Residual warrant required for some other interferences with privacy**
>
> A law enforcement agency must obtain a residual warrant if, in order to obtain evidential material relating to an offence, the agency wishes to use a device (other than a surveillance device as defined in section 3), or a technique, procedure, or activity that may constitute an intrusion into the reasonable expectation of privacy of any person.

2.31 One of the Cabinet Papers preceding the Bill noted that the residual warrant regime would reinforce the principle that "any law enforcement intrusion on reasonable expectations on privacy should generally only be permitted pursuant to warrant".[34]

2.32 The residual warrant regime was taken from the Law Commission's Report *Search and Surveillance Powers*.[35] The Report recommended that a residual regime be enacted to authorise the use of devices that interfere with reasonable expectations of privacy, but which are not otherwise subject to regulation.[36] Residual warrants would only be issued by a judge, who would need to be satisfied that the same thresholds for issuing a surveillance device warrant were met. The judge would need to prescribe in detail the scope of action that could be taken pursuant to the warrant.

2.33 A residual regime was considered desirable because of the limitations of the surveillance device warrant regime discussed above – namely, that it only covers the use of interception, tracking and visual surveillance devices in certain situations.[37] The regime did not address the lawfulness of using other devices to carry out surveillance, or the lawfulness of carrying out surveillance without a device.

---

33 Search and Surveillance Bill 2009 (45-1), cl 57.

34 Cabinet Business Committee "Law Commission Report Search and Surveillance Powers: Paper 2: Interception and Surveillance" (14 March 2008) CBC (08) 85 at [47].

35 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.121]–[11.143] and recommendations 11.24–11.26.

36 Recommendation 11.24.

37 At [11.121].

2.34 The Commission explained the advantages of the proposed residual warrant regime in these terms:[38]

> … [the residual regime] reinforces the presumptive requirement that all search, seizure, interception and surveillance activity be conducted pursuant to warrant, with the protections that attend warrants; it reinforces the rule of law; it provides enforcement officers with a means to seek authorisation for proposed law enforcement activities; it would in all likelihood reduce the number of challenges to such activities during subsequent criminal trials; it reinforces the human rights consistency principle that is central to law enforcement relationships with the wider community; and it provides enforcement officers with a measure of certainty as to the lawfulness of deploying novel techniques and devices.

2.35 The residual regime proposed in the Commission's Report was based on an existing regime in Canada, with some modifications. The Canadian regime provides for (but does not require) warrants to use devices or investigatory techniques that, if not authorised, would constitute an unreasonable search or seizure.[39]

2.36 As introduced, the Bill largely reflected the Commission's recommendations except that the residual warrant provisions were not limited to devices. The Bill would have required enforcement officers to obtain a residual warrant before using any device, technique, procedure or activity that might constitute an intrusion into the reasonable expectation of privacy of any person to obtain evidential material relating to an offence.[40]

2.37 However, during the Select Committee process concerns were raised by submitters that the regime would create a category of surveillance techniques that would not be subject to defined limits.[41] In other words, there was unease that judges would be able to authorise any type of surveillance activity they considered appropriate in the circumstances (provided the relevant criteria were met). As a result, the Bill was revised and residual warrants were replaced with declaratory orders.[42]

2.38 Declaratory orders cannot authorise otherwise illegal conduct or render it lawful. They permit a judge to indicate whether conduct is considered to be lawful and reasonable under the existing legislation and common law. They are also optional: enforcement

---

38 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.131].

39 Criminal Code RSC 1985 c C-46, s 487.01.

40 Search and Surveillance Bill 2009 (45-1), cl 57.

41 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [306].

42 As above at [305]–[314]; Search and Surveillance Bill 2010 (45-2), cls 57–61.

agencies are not required to obtain declaratory orders whenever an activity might invade a reasonable expectation of privacy.

2.39 The then Minister of Justice, the Hon Judith Collins, explained the effect of the declaratory order regime in the following terms:[43]

> The declaratory order regime allows enforcement officers to ask the court to examine the new technique, device, or activity for its reasonableness prior to using it to investigate criminal activity. … Declaratory orders could never be used to give an agency using a new surveillance device or technology the authority to trespass. The value of the declaratory order regime relates primarily to situations not involving trespass where the reasonableness of the use of a new technology or device should be considered.

2.40 The declaratory order regime was the subject of considerable debate in the House. Labour representatives questioned the appropriateness and utility of the orders, given they were only advisory in character. Charles Chauvel MP criticised the orders on the basis that:[44]

- a subsequent court dealing with the legality of the search on its facts may feel unable to depart from the indication in the order, particularly if the matter comes before the District Court and the order was made by a High Court judge;
- it was inconsistent with the judicial role and the doctrine of separation of powers to require judges to provide advice to the Executive; and
- given the order is advisory only and a subsequent court is entitled to reach a different view, it was unclear when the regime would be used and what comfort it would give to enforcement agencies.

2.41 David Parker MP noted that the orders would be very narrow in application given that they could only be used in relation to non-trespassory procedures.[45]

HOW THE LAW HAS BEEN OPERATING IN PRACTICE

2.42 We understand from our discussions with enforcement agencies that the declaratory order regime has only been used once since the Act came into force.[46] Among the

---

43 (22 March 2012) 678 NZPD 1245.

44 (7 March 2012) 678 NZPD 971.

45 (20 March 2012) 678 NZPD 1100.

46 We understand this order was made during the current reporting year, so the details of it are not yet available. The order was made on application by Police, so its annual report for 2016 will be required to describe the activity covered by the order, in accordance with s 172(f) of the Act.

enforcement officers we spoke to, there was a measure of uncertainty about their effect and the extent to which they could be relied on.

2.43 The limited nature of the surveillance device warrant regime and the lack of any guidance in the Act about when a search warrant should be obtained also seems to be problematic. Enforcement officers identified a range of investigatory techniques that they would like to be able to use in some circumstances, but they were unsure whether a warrant was required or could be obtained. Examples included the use of sniffer dogs to screen for drugs in public places, drones to fly over private property and thermal imaging devices to track a person's movements through private property from a helicopter.

COMPARABLE JURISDICTIONS

2.44 In the discussion that follows, we compare the approach taken in the Act to the law in the United Kingdom, Australia and Canada. The purpose of this comparison is to illustrate some alternative approaches, to assist in identifying options for reform.

United Kingdom

2.45 In the United Kingdom, as in New Zealand, there is no general requirement to obtain a warrant before carrying out searches or surveillance. However, the admissibility of evidence can be challenged under section 78 of the Police and Criminal Evidence Act 1984 (UK) if it was obtained in breach of article 8 of the European Convention on Human Rights.[47] This provides an incentive for law enforcement agencies to obtain authorisation if in doubt about the lawfulness of an intended course of action.

2.46 Article 8 provides that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

2.47 In assessing whether article 8 is engaged, the courts conduct a case-by-case assessment of whether the subject matter of the activity in question relates to a

[47] Convention for the Protection of Human Rights and Fundamental Freedoms 213 UNTS 221 (opened for signature 4 November 1950, entered into force 3 September 1953).

person's private life. Private life is "a broad term not susceptible to exhaustive definition".[48] A person's reasonable expectation of privacy may be a significant factor, but is not necessarily conclusive.[49] The courts have recognised there is "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'".[50]

2.48 While the position in the United Kingdom in regard to when an action may breach article 8 appears no more certain than the test under section 21 of NZBORA, the United Kingdom legislation is somewhat more thorough in terms of the activities that can be authorised. Across three different statutes there are authorisation regimes in place for:

- searches of premises, people and vehicles;[51]
- interference with property or wireless telegraphy;[52]
- interception of communications;[53]
- access to "communications data";[54]
- "directed" surveillance (surveillance for the purpose of a specific investigation that is likely to result in the obtaining of private information about a person);[55]
- "intrusive" surveillance (surveillance relating to anything taking place on residential premises or in a private vehicle, whether by a device or the presence of an individual);[56] and
- use of "covert human intelligence sources" (people who are induced, asked or assisted to create or use relationships with others to obtain information covertly).[57]

---

48 *Peck v United Kingdom* (2003) 36 EHRR 41 (Section IV, ECHR) at [57].

49 *PG and JH v United Kingdom* (44787/98) Section III, ECHR 25 September 2001 at [57].

50 *Peck v United Kingdom*, above n 48, at [57].

51 Police and Criminal Evidence Act 1984 (UK). For example, see ss 1 and 8.

52 Police Act 1997 (UK), s 93. "Wireless telegraphy" is defined in s 116 of the Wireless Telegraphy Act 2006 (UK) as the emitting or receiving of electromagnetic energy (not exceeding 3,000 gigahertz).

53 Regulation of Investigatory Powers Act 2000 (UK), s 5.

54 Section 22. Communications data includes traffic data (such as the source of a communication and how it is transmitted), non-content information about the use of a telecommunications or postal service by a person, or other information held by a service provider about a customer: s 21(4) and (6).

55 Sections 26(2) and 28(2)–(3).

56 Sections 26(3) and 32(1).

2.49 Compared to the Search and Surveillance Act in New Zealand, the United Kingdom regime covers a wider range of surveillance activity because it is not restricted to the use of particular devices. Instead, the focus is on the outcome sought or type of information that will be accessed as a result of the surveillance. In the case of directed surveillance, private information about a person is sought. In the case of intrusive surveillance, the information sought relates to what is occurring on residential premises or in a private vehicle.

2.50 An approach that focuses on the information sought rather than the method by which it is obtained is likely to respond more readily to changes in technology, as it does not depend on the functionality of particular equipment. It does, however, assume that intrusiveness depends largely on the nature of the information sought rather than the way in which it is obtained.

2.51 Compared to New Zealand, the United Kingdom regime may provide greater certainty for law enforcement agencies and their oversight bodies, since it allows authorisation to be granted for a wider range of activity. It may also provide greater assurance to the public that there is a sufficiently detailed framework in place for authorisation of investigatory activity.

2.52 On the other hand, there is an argument that the United Kingdom regime is less transparent about the actual activities of enforcement agencies, since the focus is on the outcome sought or information likely to be obtained rather than the exact method or device that will be used.

Australia

2.53 In Australia there is also no general requirement to obtain a warrant. Warrant provisions are empowering rather than mandatory. As in New Zealand, certain investigatory activities will be unlawful if they have not been authorised under a warrant, such as conduct involving trespass or the interception of communications passing over a telecommunications system.[58] However, the legal status of other unwarranted investigatory activities is more ambiguous (for example, some non-trespassory uses of surveillance devices).

---

[57] Regulation of Investigatory Powers Act 2000 (UK), ss 26(7)–(8) and 29.

[58] Telecommunications (Interception and Access) Act 1979 (Cth), s 7(1).

2.54 Australia does not have a Bill of Rights, so there is no equivalent to section 21 of NZBORA. Australia has ratified the International Covenant on Civil and Political Rights (ICCPR),[59] article 17 of which provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

2.55 The ICCPR is not directly enforceable in Australia. However, if conduct breaches a right recognised in the ICCPR, that will be a factor in determining whether evidence obtained as a result of the conduct should be excluded from subsequent proceedings.[60]

2.56 The scope of the legislation authorising search and surveillance activity in Australia is broadly comparable to New Zealand. The Crimes Act 1914 (Cth) provides for the issuing of search warrants in relation to premises or people[61] and sets out some warrantless search powers.[62] There is also some State legislation containing search powers, which we have not canvassed in this Paper.

2.57 Interception of communications is governed by the Telecommunications (Interception and Access) Act 1979 (Cth). The offence of intercepting communications is slightly broader in Australia than in New Zealand, in that it does not require the use of a "device" and applies to any communication (not just private communications).[63] As a result, the warrant provisions are also broader. Law enforcement agencies can obtain interception warrants either in relation to a telecommunications services provider[64] or in respect of the communications of a particular person.[65]

2.58 Aside from interception, the Australian surveillance regime provides an authorisation process only for the use of specific types of surveillance devices.[66] These are listening

---

59 International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976).

60 Evidence Act 1995 (Cth), s 138(3)(f).

61 Crimes Act 1914 (Cth), s 3E.

62 See for example Crimes Act 1914 (Cth), s 3T (searches of conveyances in emergency situations) and Division 3A (powers in relation to terrorist acts and terrorism offences).

63 Telecommunications (Interception and Access) Act 1979 (Cth), ss 6(1) and 7(1).

64 Section 46.

65 Section 46A.

66 Surveillance Devices Act 2004 (Cth), s 10.

devices, tracking devices, optical surveillance devices and data surveillance devices.[67] "Data surveillance device" does not have an equivalent in the Search and Surveillance Act. It is defined as any "device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer".[68] This would appear to include, for example, keystroke logging.[69]

2.59 In summary, while the interception and surveillance device warrant regimes are slightly broader in Australia than in New Zealand, the overall framework is similar. There is no general requirement to obtain a warrant and the authorisation regime does not cover surveillance without the use of a device (with the exception of communications interception).

Canada

2.60 The Canadian regime contains comparatively few types of warrants or authorisations and instead takes a more generic approach. There is provision for judges to issue warrants permitting law enforcement officers to search a building, place or receptacle;[70] intercept private communications;[71] or use a tracking device[72] or transmission data recorder.[73] Authorisation of any other law enforcement search or surveillance activity (for example, video surveillance) occurs under a "general warrant".

2.61 Historically, the term "general warrant" was used in the common law to refer to warrants that conferred broad discretion on a law enforcement officer to search unspecified people or places, and for unspecified things. These warrants were treated as invalid because they did not sufficiently identify what could be done by the person executing them.[74]

---

67 Surveillance Devices Act 2004 (Cth), s 6 (definition of "surveillance device").

68 Section 6 (definition of "data surveillance device").

69 Keystroke logging refers to the use of a software program to monitor keystrokes that a user types on a computer's keyboard.

70 Criminal Code RSC 1985 c C-46, s 487(1).

71 Sections 184.2 and 186. There is also a warrantless power for police officers to intercept private communications to prevent serious imminent harm (s 184.4).

72 Section 492.1.

73 Section 492.2. A transmission data recorder is a device that records certain metadata relating to communications (but not their content) – for instance the date, time and duration of a communication. See s 492.2(6), definitions of "transmission data" and "transmission data recorder".

74 See the discussion in *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [15]–[16].

2.62 Despite its name, the Canadian general warrant regime requires specificity about the investigatory methods to be used, the object of the search and the offence it relates to.[75] It permits a judge to authorise an enforcement officer to:[76]

> … use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property.

2.63 Before issuing a general warrant, the judge must be satisfied that:[77]

- there are reasonable grounds to believe an offence has been or will be committed and that information concerning the offence will be obtained through the use of the technique proposed;
- it is in the best interests of the administration of justice to issue the warrant; and
- there is no other provision that would provide for a warrant or authorisation permitting the technique to be used.

2.64 The Act enables the issuing of general warrants, rather than requiring them to be obtained before conducting activity that may otherwise amount to an unreasonable search or seizure. However, any unreasonable search or seizure would be captured by section 8 of the Canadian Charter of Rights and Freedoms 1982 (the equivalent of section 21 of NZBORA), which provides that "[e]veryone has the right to be secure against unreasonable search or seizure". In determining what amounts to a "search" under section 8, the Canadian courts apply the "reasonable expectation of privacy" test that has now been adopted in New Zealand.[78]

2.65 The Supreme Court of Canada held in *Hunter v Southam Inc* that any search without a warrant is presumptively unreasonable.[79] Dickson J, giving the judgment of the Court, said:[80]

> That purpose [of section 8] is, as I have said, to protect individuals from unjustified state intrusions upon their privacy. That purpose requires a means of *preventing* unjustified searches before they

---

75 Criminal Code RSC 1985 c C-46, s 487.01(1) and (5). Section 487.01(5) applies s 184.2 (which relates to interception) with any necessary modifications. Section 184.2(4) requires a warrant to specify the relevant offence, the information sought and the identity of the target person.

76 Section 487.01(1).

77 As above.

78 *R v Wise* [1992] 1 SCR 527 at 533; *Hunter v Southam Inc* [1984] 2 SCR 145 at 159.

79 *Hunter v Southam Inc*, above n 78, at 161.

80 At 160–161 (original emphasis).

> happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in my view, can only be accomplished by a system of *prior authorization*, not one of subsequent validation.
>
> A requirement of prior authorization, usually in the form of a valid warrant, has been a consistent prerequisite for a valid search and seizure both at common law and under most statutes. Such a requirement puts the onus on the state to demonstrate the superiority of its interest to that of the individual. As such it accords with the apparent intention of the *Charter* to prefer, where feasible, the right of the individual to be free from state interference to the interests of the state in advancing its purposes through such interference.
>
> I recognize that it may not be reasonable in every instance to insist on prior authorization in order to validate governmental intrusions upon individuals' expectations of privacy. Nevertheless, where it is feasible to obtain prior authorization, I would hold that such authorization is a precondition for a valid search and seizure.

2.66 If evidence is found to have been obtained in a manner that infringes section 8 (for example, because a warrant was not obtained when it ought to have been), it may be excluded from proceedings.[81]

2.67 In combination, the case law requiring pre-authorisation and the general warrant regime in the Criminal Code mean that law enforcement officers are generally required to obtain a warrant before carrying out a search or any kind of surveillance activity. Evidence obtained through methods that invade a reasonable expectation of privacy without a warrant is likely to be excluded in subsequent proceedings.

2.68 The Canadian authorisation regime is probably the broadest (in terms of the types of activity captured) of those examined. However, it still has weaknesses. These include:

- The general warrant regime is only engaged if the proposed activity may constitute an *unreasonable* search or seizure. This suggests law enforcement officers need not seek a warrant to carry out a search if they consider the intrusion on an individual's expectations of privacy will be reasonable. Arguably law enforcement officers are not in the best position to make this assessment, and pre-authorisation should be sought for any search.
- The requirement to obtain a warrant—established in Canadian case law—is not reflected in legislation. This may not provide the same level of transparency and assurance to the public as a statutory requirement. However, it still provides a strong incentive for enforcement officers to seek a general warrant if they are in

[81] Canadian Charter of Rights and Freedoms 1982, s 24(2).

any doubt, to give them confidence that they are acting lawfully and that any evidence obtained is likely to be admissible.

- A residual warrant can only be issued where there is no other warrant or authorisation available for the type of technique or device in question.[82] This appears to have resulted in some uncertainty in practice. There may be borderline cases where it is not clear to an enforcement officer whether a particular technique can be authorised under another type of warrant.[83]

COMPARABLE LEGISLATION IN NEW ZEALAND

2.69 A comparison can also be drawn with the search and surveillance authorisation regime used by New Zealand's intelligence and security agencies – the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS). While these agencies exercise their powers for different purposes than law enforcement agencies (that is, for national security and intelligence collection purposes) some of their activities are similar.

2.70 The legislation governing NZSIS and GCSB was the subject of a recent independent review by Sir Michael Cullen and Dame Patsy Reddy.[84] A Bill to replace the existing legislation with a new Act was introduced on 15 August 2016.[85] The Bill has now been referred to the Foreign Affairs, Defence and Trade Committee, which is due to report back to Parliament on 18 February 2017.

2.71 Under the current law, NZSIS can obtain intelligence warrants allowing them to undertake electronic tracking or to intercept or seize any communication, document, or thing not otherwise lawfully obtainable.[86] Following amendments in 2014 to address the threat of foreign terrorist fighters, NZSIS can now also obtain a warrant authorising visual surveillance.[87] The warrant provisions in the New Zealand Security Intelligence Service Act 1969 are empowering rather than mandatory.

---

82 Criminal Code RSC 1985 c C-46, s 487.01(1)(c).

83 See for example *R v TELUS Communications Co* [2013] 2 SCR 3.

84 Sir Michael Cullen and Dame Patsy Reddy *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security* (29 February 2016).

85 New Zealand Intelligence and Security Bill 2016 (158-1).

86 New Zealand Security Intelligence Service Act 1969, s 4A.

87 New Zealand Security Intelligence Service Act 1969, s 4IB (inserted by the New Zealand Security Intelligence Service Amendment Act 2014).

2.72 The Government Communications Security Bureau Act 2003, on the other hand, expressly provides that GCSB can only undertake certain activities using an interception device or access an information infrastructure[88] with authorisation under the Act.[89] The Act then provides for interception warrants, authorisations to access information infrastructures[90] and a limited warrantless interception power.[91]

2.73 The Cullen/Reddy review identified a number of gaps in the authorisation regimes applying to GCSB and NZSIS. The reviewers explained:[92]

> Many of the NZSIS's activities rely on the fact that something is not otherwise unlawful – for instance, carrying out surveillance in public places. Under the GCSB legislation, interception warrants are only required for interception using particular methods. This results in uncertainty for both the Agencies and the public. Given the intrusive nature of the Agencies' activities, we consider all of their powers should be subject to an authorisation regime.

2.74 The reviewers went on to recommend a new authorisation regime that would "require some form of authorisation for all of the Agencies' intelligence and security activities that involve gathering information about individuals and organisations".[93] Activities that are generally lawful, such as surveillance in public places or accessing publicly available information, would be governed by a policy statement issued by the responsible Minister rather than by a warrant.[94]

2.75 These recommendations are largely reflected in the Bill, with some modifications. Clause 49 provides that NZSIS and GCSB may only carry out activity that is otherwise unlawful if it is authorised by a warrant or authorisation.[95] Clause 63 of the Bill exhaustively lists the otherwise unlawful activities that can be authorised. The Bill also allows for the issue of ministerial policy statements to provide guidance to NZSIS and GCSB on the exercise of their lawful powers.[96]

---

88 Information infrastructure is defined broadly as including electromagnetic emissions, communications systems and networks, information technology systems and networks, and any communications carried on, contained in, or relating to those emissions, systems, or networks. See the Government Communications Security Bureau Act 2003, s 4.

89 Government Communications Security Bureau Act 2003, s 15.

90 Section 15A.

91 Section 16.

92 Cullen and Reddy *Intelligence and Security in a Free Society*, above n 84, at [6.7].

93 Recommendation 41.

94 Recommendations 50–51.

95 New Zealand Intelligence and Security Bill 2016 (158-1), cl 49(1).

96 Clauses 165–174.

2.76 The Bill provides an example of a relatively prescriptive authorisation regime (similar to the third option we discuss below[97]). It remains to be seen whether NZSIS and GCSB will encounter similar problems to enforcement officers under the Act in determining what is "otherwise unlawful". Ministerial policy statements may assist by clarifying what the agencies' lawful powers are (although, as with declaratory orders under the Act, these policy statements will not be able to authorise unlawful activity).

THE CASE FOR REFORM

2.77 As discussed above, the current approach in the Act is to require a warrant only for the use of particular surveillance devices. Otherwise, enforcement officers determine whether a warrant should be sought based on the reasonable expectation of privacy test.

2.78 Throughout this chapter we have noted some potential problems with this approach:

- Our initial consultation suggests the current regime does not provide sufficient flexibility to ensure enforcement agencies can make use of new technologies. This may prevent them from doing their jobs in the most efficient and effective way possible.
- The concept of a reasonable expectation of privacy can be difficult for enforcement officers to apply. This creates uncertainty about when they need to obtain a warrant and whether certain methods can be used at all.
- The current approach does not provide legislative assurance that the privacy interests at stake will always be independently assessed before intrusive activity is carried out. In some cases, the legality and reasonableness of an investigatory technique is only considered by a court after-the-fact if the admissibility of evidence is challenged.[98] Even then, evidence obtained from an illegal search may still be admissible.[99]

2.79 While the Act provides for declaratory orders to address the use of techniques not explicitly anticipated by the authorisation regime, seeking such an order is optional.

---

97 See paragraphs [2.102]–[2.104].

98 See for example *Lorigan v R*, above n 9; *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753; *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204; and *R v Wilson* [2015] NZSC 189, [2016] 1 NZLR 705.

99 For some recent examples of cases where evidence obtained through unlawful searches was deemed admissible under section 30 of the Evidence Act 2006, see *Rihia v R* [2016] NZCA 200 and *Birkinshaw v R* [2016] NZCA 220.

The orders are indicative only so they may not provide enforcement officers with a high level of certainty that they are acting lawfully. They also cannot authorise conduct that is unlawful (for example, conduct involving trespass that is not permitted by legislation). Enforcement agencies cannot use new methods falling under that category unless and until the Act is amended by Parliament.

2.80 For example, if Police wished to covertly install a thermal imaging device on private property to monitor the heat output of a garage for signs of cannabis growing, that would involve trespass. None of the current warrant provisions in the Act would appear to cover this type of activity, since the surveillance regime is limited to specific devices. Police may be unable to proceed, even though the Act does allow authorisation of much more intrusive activity (such as visual surveillance on private property and interception of private communications).

2.81 Enforcement agencies told us that the current situation lacks certainty. It is not always clear whether a warrant is required (or even available) and the extent to which new investigatory methods can be lawfully used. This uncertainty could become more pronounced as technology advances further beyond what was originally anticipated by the Act and enforcement agencies seek to develop their investigatory methods accordingly.

2.82 In our view, this uncertainty is arguably undesirable from the perspective of members of the public as well. The Act may not provide a sufficiently high degree of assurance that privacy interests are being adequately and proactively protected.

OPTIONS FOR REFORM

2.83 As is apparent from the various approaches taken in other jurisdictions and the legislation governing intelligence agencies, there are a number of different ways in which the scope of an authorisation regime can be framed. We set out below two broad options:

- retain the status quo; or
- clarify when a warrant should or must be obtained (we suggest three ways in which that might be done).

2.84 If it is considered desirable to clarify when a warrant should or must be obtained, any of the three options we suggest would also require the Act to define the type of conduct for which authorisation should be sought. We discuss two possible definitions.

Retain the status quo

2.85 One option is to retain the current approach of a largely permissive (rather than mandatory) warrant regime and provision for declaratory orders. Despite the problems discussed above, there are some advantages to this approach.

2.86 Because the declaratory order regime cannot authorise activity that is unlawful, in one sense it provides a relatively high degree of individual rights protection. Only Parliament (through amendments to the Act) can decide to permit novel techniques that would otherwise breach the law or constitute an unreasonable search. This ensures that any extension of the law to cover new investigatory techniques is carefully considered.

2.87 The current approach also provides a reasonable degree of flexibility for enforcement agencies to use new methods that are permissible under general law. Because the Act does not restrict enforcement agencies to carrying out only those search and surveillance activities that are expressly authorised under the Act, novel investigatory methods can be pursued if they will not breach section 21 of NZBORA or another rule of law (such as trespass). Declaratory orders are able to provide some degree of assurance about the reasonableness of new methods.

2.88 If this approach is retained, it would still be possible to revise the scope of the surveillance device warrant regime to reduce gaps in the regime. In other words, the Act could be amended to include additional types of surveillance devices (or even types of surveillance without a device) within the list of surveillance activities that require a warrant. This could help to address some of the problems identified with the current approach, without changing the overall structure of the Act. This option is discussed in more detail in Chapter 3.

Clarify when a warrant should or must be obtained

2.89 We discuss below three possible alternatives to the current approach, which could help to clarify when a warrant should or must be obtained:

- *Option 1:* introduce a residual warrant regime without expressly requiring authorisation for all search and surveillance activity.
- *Option 2:* require authorisation for all search and surveillance activities and introduce a residual warrant regime.
- *Option 3:* require authorisation for all search and surveillance activities, without introducing a residual warrant regime.

2.90 If option 2 or option 3 were adopted, the legislation would need to define what type of conduct requires authorisation (in other words, what a "search" or "surveillance" is). This could be based on the reasonable expectation of privacy test applied under section 21 of NZBORA, or a different threshold may be appropriate. This is discussed in more detail below (see paragraph 2.105 onward). Consideration would also need to be given to the consequence of failing to comply with the requirement to obtain a warrant.

2.91 If option 1 were adopted, the legislation would need to identify when a residual warrant could be sought. Given the regime would not be mandatory the test would be less crucial than for options 2 and 3, but it would still play an important role in setting expectations about when the regime should be used.

Option 1: Introduce an optional residual warrant regime

2.92 This option would involve replacing the current declaratory order provisions with a residual warrant regime similar to the Canadian example.[100] Enforcement officers would be able to seek pre-authorisation from a High Court judge for investigatory methods not covered by specific authorisation provisions. The warrant would still need to be specific about the type of activity authorised and the evidential material sought.

2.93 There would be no general requirement to obtain authorisation for all searches, so it would still fall to enforcement officers to determine whether it is necessary to seek a warrant. However, there would be a clear incentive to seek a warrant in borderline cases, as a warrant may provide a greater degree of certainty to enforcement officers (compared to declaratory orders) that they are acting lawfully and that any evidence obtained is likely to be admissible.[101]

2.94 A residual warrant regime may be more effective at allowing the legislation to adapt to technological developments. It could enable enforcement agencies to use the most effective and efficient tools available to them, provided a judge is first satisfied that the proposed activity is necessary and proportionate in the circumstances.

2.95 This approach could allow new investigatory techniques (including those that might otherwise breach the law) to be used without Parliament having expressly considered

---

[100] See above at paragraphs [2.60]–[2.68] of this Issues Paper.

[101] It is possible for a search that is otherwise lawful to be unreasonable in terms of s 21 of New Zealand Bill of Rights Act 1990 due to the manner of execution, but this will be rare: *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [24].

them in advance. It would rely on High Court judges to decide whether the use of new methods is justified. However, detailed criteria could be put in place to guide that decision. For example, judges could be required to weigh the level of intrusion on privacy against the seriousness of the offending and evidence likely to be obtained, and consider whether the activity is proportionate.

2.96 If there was concern about new techniques being authorised on an ex parte basis (that is, without hearing arguments on both sides), the Act could provide for the appointment of an amicus curiae[102] to advise the court on the potential rights implications. Judges would also be able to impose conditions to minimise the level of intrusion on rights.

Option 2: Introduce a mandatory residual warrant regime

2.97 This option would resemble the approach in the Search and Surveillance Bill when it was introduced. Enforcement agencies would be required to obtain a residual warrant from a High Court judge before carrying out any search or surveillance activity not specifically authorised elsewhere in legislation.

2.98 There would continue to be specific warrants and powers in the Act in relation to relatively common investigatory techniques (such as those currently covered by warrants under the Act). However, the residual regime would apply in relation to any relevant conduct falling outside those specific provisions.

2.99 This option is similar to option 1 in a number of respects. It would allow enforcement agencies to use new methods without requiring amendments to the Act and could provide detailed criteria to guide the judge's decision. The warrant would need to be specific about the activity permitted and the evidential material sought. As with option 1, the appointment of amicus curiae could also be considered.

2.100 However, unlike option 1, the mandatory nature of this option would help to ensure that the likely impact of an activity on individuals is assessed by a High Court judge in all appropriate cases. In addition to providing a higher level of protection of individuals' privacy rights, this may help to reduce subsequent challenges to the admissibility of evidence in criminal trials.

---

[102] Amicus curiae means "friend of the court". An amicus can be appointed by a court to provide impartial advice on an aspect of the law or to advance legal arguments on behalf of a party who is not represented by legal counsel. He or she does not act on instructions from a party to the proceeding.

2.101 In theory, this option could also provide a higher degree of certainty to enforcement officers than the current regime does in relation to when a warrant is required. However, it may be difficult to come up with a sufficiently clear test for determining when authorisation must be sought. If the test is unclear or difficult to apply in practice, this could result in issues similar to those arising now: enforcement officers would be left to make judgement calls about whether or not to seek a warrant. The residual warrant regime would at least mean that enforcement officers would have the option to seek a warrant if they are uncertain, which is not always the case currently.

Option 3: Require specific authorisation for all search and surveillance activities

2.102 Under this option, warrants would continue to be available only in relation to specified types of activity. However, the Act would expressly restrict enforcement agencies to only carrying out search or surveillance activity that is authorised by legislation.

2.103 This approach would provide a relatively high level of protection for privacy rights, as it would:

- require judicial authorisation in advance of all search or surveillance activity, unless an express exception is recognised in legislation; and
- ensure that particular search and surveillance methods are only used if Parliament has expressly considered them and endorsed their use in legislation.

2.104 However, the lack of flexibility in this approach is highly likely to result in enforcement agencies not having access to the most effective investigatory tools as technology develops. Regular amendments would be required to ensure the Act allows for all appropriate methods, which would be time-consuming and costly for government.

Q1 Should the Act be more specific about when a warrant (or specific search power) is required?

Q2 Should the declaratory order regime in the Act be replaced with a residual warrant regime, allowing a High Court judge to authorise activity not captured by a specific warrant or power?

Define the conduct that requires authorisation

2.105 As noted above, either of options 2 or 3 would require the legislation to define the type of conduct for which authorisation must be obtained. If option 1 were adopted, the legislation would still need to set out when a residual warrant could be sought. This section discusses whether the reasonable expectation of privacy test is the right one in this context, or whether an alternative test should be considered.

2.106 It is important to be clear that in referring to conduct requiring authorisation, we do not mean a warrant would be required for all activity meeting the relevant test. Authorisation might be by statute. For example, the Act (or, for non-Police enforcement agencies, other legislation) could create warrantless powers or exceptions to the requirement to obtain a warrant (such as for consent searches). Alternatively, a different type of authorisation could be required, such as authorisation by the Commissioner of Police for activities that involve a lesser degree of intrusion, or government policy statements in relation to certain classes of activity.

Current test: conduct that invades a reasonable expectation of privacy

2.107 Currently, in deciding whether an authorisation is required, enforcement agencies by default apply the reasonable expectation of privacy test adopted by the courts under section 21 of NZBORA.

2.108 That test has also been adopted in the declaratory order regime. Under section 66 of the Act, an enforcement officer can apply for a declaratory order if they wish to carry out activity that:

- is not specifically authorised by another statutory regime; and
- may constitute an intrusion into the reasonable expectation of privacy of any other person.

2.109 Some benefits of using the reasonable expectation of privacy test are:

- it would be consistent with the approach taken under section 21 of NZBORA and in some other jurisdictions (such as Canada);
- there is already case law on how the test should be applied; and
- enforcement officers are already familiar with the test.

2.110 However, as we have discussed above, there is some uncertainty about how the test operates in practice. There are also concerns that the test may lead to a progressive reduction in the level of protection of privacy rights if practices and technologies that compromise privacy interests become more commonplace.

2.111 The reasonable expectation of privacy test was adopted by the courts for the purpose of determining when a right has been breached. It is not necessarily the appropriate test for determining when pre-authorisation of investigatory activity is required. In the context of the Act, enforcement officers rather than judges are required to make this assessment in the first instance. Given the test is a complex one to apply, enforcement

officers may not be well-placed to do that. If the assessment is made incorrectly, it may lead to important rights being breached and prosecutions failing as a result of crucial evidence being excluded.

An alternative test: conduct that might engage privacy interests

2.112 A lower and more certain threshold could be considered, to ensure that pre-authorisation is sought whenever privacy interests *might* be engaged. This would mean that complex assessments of whether proposed activity is justified in light of the opposing interests at stake would, in general, be left to issuing officers (except where warrantless powers or lower-level authorisations have been expressly provided for by Parliament).

2.113 A lower threshold could well result in an increased number of warrant applications, which would have resourcing implications for both enforcement agencies and issuing officers. However, if the aim of increasing the certainty of the test was achieved, it could also reduce the number of challenges to the admissibility of evidence in subsequent criminal proceedings.

2.114 Creating an appropriate test is likely to be difficult. If the test is too narrow it would not adequately protect privacy rights. If it is too broad, it would reduce the responsiveness of enforcement agencies by requiring them to obtain a warrant in cases where that may not be justified. Any alternative test would need to be carefully worked through to ensure it appropriately balances human rights and law enforcement values. We welcome any comments that may assist in achieving that balance.

2.115 We provide one possible—but very preliminary—example of an alternative test below for the purpose of promoting discussion. As we have noted,[103] we do not suggest it would be appropriate to require enforcement officers to obtain a warrant for all conduct falling within this definition. Rather, it would provide a default position that would need to be subject to specific warrantless powers or exceptions (which might include, for example, an internal form of authorisation for some activities).

2.116 In addition, if there is support for including a definition of this kind in the Act, we would need to consider how it would apply across a range of circumstances. We

---

[103] See paragraph [2.106] above.

would particularly like to hear from submitters about any practical situations they can think of where the example test below might lead to undesirable outcomes.

2.117 The Act could require authorisation (or enable a residual warrant to be sought) for:

> … any activity by an enforcement officer that is either intended to result, or can reasonably be foreseen as likely to result, in the obtaining of:
>
> (a) information relating to an identifiable person; or
>
> (b) evidential material of any kind;
>
> in circumstances where—
>
> (a) the information is not publicly available; or
>
> (b) but for the use of a technological aid, the information could only be obtained by searching a place, vehicle, person or thing (including computers and devices) that the enforcement officer is not lawfully entitled to access.

2.118 Thought would need to be given to how "publicly available" would be defined. One option would be to take into account the nature and quantity of the information obtained and how it will be used. For example, camera footage taken by a police officer in the street during an incident may be comparable to footage that could be taken by a member of the public, so would not require authorisation. However, systematic CCTV surveillance across a city would be substantially different in character, particularly if it could be:

- used to track an individual's movements; or
- linked with facial recognition software and cross-referenced against a police database to identify wanted people.

2.119 Similarly, an operation that involves following an individual for an extended period of time might require authorisation of some kind. This is because it may disclose significantly more information about that person than would be apparent to a member of the public going about their ordinary business.

2.120 The "use of a technological aid" limb is intended to ensure that the protection afforded by the Act is not eroded as more advanced technologies become publicly accessible. It would capture the use of commonly available devices to gain access to information that could otherwise only be obtained through trespass or other unlawful activity.

2.121 The example test given above is based primarily on a distinction between information that is publicly available and information that is not. It would leave little scope for recognition of privacy in what a person does in public view, unless (as noted above in the CCTV example) the search or surveillance methods used disclose a significantly

greater level of information than an ordinary person would be able to obtain. For example, a conversation held in a public place is unlikely to be caught by the definition because any passer-by could hear it.

2.122 This approach is broadly consistent with the view taken by the majority of the Supreme Court in *Hamed v R.*[104] That case concerned the legality of police search and surveillance activities carried out in the Urewera Ranges during an investigation into suspected terrorist activities. Police obtained a number of search warrants in order to gather evidence of military-style training camps occurring on Tūhoe-owned land. The activities carried out in reliance on the warrants included video surveillance both on the Tūhoe-owned land and on a public road near the entrance to that land.

2.123 In considering whether the public video surveillance was a search under section 21 of NZBORA, Blanchard J (with whom the majority agreed) said:[105]

> If the surveillance is of a public place, it 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. People in the community do not expect to be free from the observation of others, including law enforcement officers, in open public spaces such as a roadway or other community-owned land like a park, nor would any such expectation be objectively reasonable. The position may not be the same, however, if the video surveillance of the public space involves the use of equipment which captures images not able to be seen by the naked eye, such as the use of infra-red imaging.

2.124 The Chief Justice took a contrary view, stating that "[i]f those observed or overheard reasonably consider themselves out of sight or earshot, secret observation of them or secret listening to their conversations may well intrude upon personal freedom".[106] The example test we have outlined above may not provide this level of privacy protection (depending on how "publicly available" is defined).

2.125 There is an argument that actions by enforcement agencies should be more strictly controlled than comparable actions by members of the public. This is because the information can be used by enforcement agencies in different ways (due to the tools and other information available to them) and may lead to serious consequences (such

---

104 *Hamed v R*, above n 9. The Court in *Hamed* (which was decided pre-Search and Surveillance Act) unanimously found that the law at that time did not permit the issuing of prospective or anticipatory warrants, so video surveillance could not be authorised (at [6], [145]–[150] and [210]–[213]). As a result of this finding, the Government urgently enacted the Video Camera Surveillance (Temporary Measures) Act 2011. That Act allowed (with retrospective effect) the use of covert video surveillance as part of a search pending the enactment of the Search and Surveillance Act.

105 At [167].

106 At [12].

as a criminal prosecution). An enforcement officer is also more likely than a member of the public to know that something they see or overhear is relevant to an investigation. On the other hand, drawing such a distinction may not be sustainable given that members of the public who observe or record evidence of offending can (and frequently do) provide information about it to enforcement agencies.

2.126 We discuss the extent to which surveillance carried out in public places should be regulated by the Act in greater detail in Chapter 3.[107]

2.127 The example test above would capture more conduct than the reasonable expectation of privacy test. Careful thought would need to be given to what specific exceptions are appropriate, to ensure that enforcement officers are not unduly constrained or required to obtain warrants for routine activity. For example, the Act might need to specifically permit enforcement officers to question suspects or obtain information from another government agency. These actions could fall within the example test if the information obtained is not public knowledge.

2.128 Finally, we note that introducing a different threshold under the Act would not alter the test applied under section 21 of NZBORA. The courts would continue to apply the reasonable expectation of privacy test in that context (or any other test adopted in case law in the future). However, as any unlawful conduct will usually be unreasonable under section 21,[108] any action taken in breach of a prohibition on unauthorised searches would also be likely to breach section 21.

Q3 What factors should determine whether or not the conduct of an enforcement officer requires a warrant or specific search power, and why? For example:

(a) that the conduct invades a reasonable expectation of privacy;

(b) that the conduct targets a particular individual;

(c) that the information the agency is seeking to obtain is not publicly available;

(d) that the information is only able to be obtained through trespass or through the use of a device or technique that discloses information about things occurring on private property.

---

[107] See paragraphs [3.104]–[3.129] below.

[108] *Hamed v R*, above n 9, at [174].