Chapter 4 – Surveillance: Interception and tracking device warrants

INTRODUCTION

4.1 This chapter looks at issues arising from the surveillance device warrant regime as it applies to interception and tracking devices. In particular, we examine whether the definitions of "private communication" and "tracking device" in the Search and Surveillance Act 2012 (the Act) need to be revisited in light of recent developments in technology.

INTERCEPTION DEVICE WARRANTS

The current law

The warrant requirement

4.2 Generally, the Act requires enforcement officers to obtain a surveillance device warrant if they wish to use an interception device to intercept a private communication.[1]

4.3 The warrant requirement stems from section 216B of the Crimes Act 1961. Under that section it is an offence to intentionally intercept a private communication by means of an interception device. The interception offence in section 216B was enacted in 1979, and was preceded by a similar provision in the Misuse of Drugs Amendment Act 1978. The definition of "private communication" in the Crimes Act was originally confined to oral communications, but was updated in 2003 to cover other forms of communication (such as emails and text messages). Otherwise it has remained largely unchanged despite significant technological developments since 1978.

4.4 The definitions of "intercept" and "private communication" in the Act[2] are based on those in the Crimes Act,[3] with some minor differences. These definitions are important in determining the scope of the warrant requirement:

---

1 Search and Surveillance Act 2012, s 46(1)(a). "Interception device" is broadly defined in s 3 as "any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept or record a private communication (including a telecommunication)" (excluding hearing aids).

2 Search and Surveillance Act 2012, s 3.

3 Crimes Act 1961, s 216A.

intercept, in relation to a private communication, includes hear, listen to, record, monitor, acquire, or receive the communication either—

(a) while it is taking place; or

(b) while it is in transit

private communication—

(a) means a communication (whether in oral or written form, or in the form of a telecommunication, or otherwise) made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but

(b) does not include a communication of that kind occurring in circumstances in which any party to the communication ought reasonably to expect that the communication may be intercepted by some other person without having the express or implied consent of any party to do so

4.5 The requirement to obtain a warrant is limited to the use of an interception *device*, so does not cover (for instance) unrecorded eavesdropping by an enforcement officer. The definition of "intercept" only applies while the communication is taking place or in transit. An interception device warrant is not required to obtain a communication after it has taken place (for example, by requesting a record of it from a telecommunications provider); instead, a production order would usually be sought for this.

4.6 The warrant requirement is also restricted to the interception of "private" communications. The definition of private communication contains two distinct limbs. The first, in paragraph (a), involves an assessment of whether the parties subjectively intended the communication to remain private. The second, in paragraph (b), involves an objective assessment of whether interception ought reasonably to be expected.

4.7 In the context of the Crimes Act, the second limb of the definition of "private communication" has been interpreted in a relatively confined way.[4] The fact that members of the public might recognise there is a theoretical risk of interception (for example, because of a general awareness that enforcement agencies can intercept cell phone calls) does not itself mean that the "private" nature of a communication is lost.[5] Rather, a perceived reasonable likelihood of interception is required.

---

4 *Moreton v Police* [2002] 2 NZLR 234 (HC). This case is discussed in greater detail below at paragraph [4.12].

5 *Moreton v Police*, above n 4, at [69]–[70].

Exceptions to the warrant requirement

4.8 The Act recognises some exceptions to the warrant requirement. A surveillance device warrant is not required:

- to make a "covert audio recording of a voluntary oral communication between 2 or more persons made with the consent of at least 1 of them";[6] or
- if the interception is authorised by an interception warrant issued under the Government Communications Security Bureau Act 2003 or New Zealand Security Intelligence Service Act 1969, or by any other enactment.[7]

4.9 The consent exception is also a reflection of the Crimes Act interception offence provisions. They recognise an exception to the offence for any party to the communication or any person who has the express or implied consent of a party to intercept the communication. The notable difference between the Crimes Act and the Search and Surveillance Act is that the Crimes Act exception can apply to any interception of private communication, whereas the exception in the Search and Surveillance Act is limited to covert audio recordings of oral communications. It is not clear that this difference was deliberate.[8]

The scope of the interception regime

4.10 The definition of "private communication" limits the scope of the interception warrant regime. The scope of the regime does not appear to have been considered in any detail by the Law Commission when preparing its 2007 Report, *Search and Surveillance Powers*. The Report simply recommended consolidating the existing statutory provisions dealing with the use of interception and tracking devices into the new surveillance device warrant regime.[9]

---

6 Search and Surveillance Act 2012, s 47(1)(b).

7 Section 47(1)(c) and (d).

8 In its Report, *Search and Surveillance Powers* (NZLC R97, 2007) at [11.76], the Law Commission only recommended an exception for the "surreptitious recording of a voluntary conversation" (which suggests an oral conversation) but noted this would "reflect the status quo" in the Crimes Act 1961 (which referred to interception of private communications generally).

9 See recommendation 11.5.

The definition of "private communication"

4.11 There is, however, an element of circularity to the definition of "private communication" that has been the subject of considerable criticism.[10] The test for what is "private" depends on whether any party to the communication "ought reasonably to expect that the communication may be intercepted".[11] This test carries with it some of the same issues as the reasonable expectation of privacy test discussed in Chapter 2. In essence, the argument is that if interception of communications by the State becomes commonplace, it will almost always be reasonable for a person to expect that their communication *may* be intercepted.

4.12 This issue was discussed in some depth by William Young J in his 2002 judgment in *Moreton v Police.* In that case a member of the public intercepted a cell phone call using a radio scanner and then reported what she had heard to New Zealand Police. The defence objected to the use of her evidence on the basis that she had unlawfully intercepted a private communication.

4.13 When considering the effect of the interception offence provisions in the Crimes Act, William Young J noted:[12]

> Since 1978 (when this language first appeared in our statute book) there have been substantial developments in technology and police practice. Accordingly, reasonable expectations as to the possibility or likelihood of interception have developed over time. Because the concept of reasonable expectation is embedded in the definition of what constitutes a "private communication" the definition appears to have an ambulatory application. In other words, with growing public awareness of the likelihood of interception, communications which once might have been "private" might no longer be able to be so regarded.

4.14 To illustrate this point, his Honour noted that it is now common in criminal trials for Police to rely on intercepted communications between people allegedly involved in drug dealing. Such communications are often in code because the parties anticipate a risk of interception. As a result, his Honour thought it was arguable that people who

---

[10] See for example *Moreton v Police*, above n 4; Legislation Advisory Committee *Submission on the Government Communications Security Bureau and Related Legislation Bill* (12 June 2013) at [26]; Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at [3.66]; and Denis Tegg "Loophole that Legalises Official Snooping" *The New Zealand Herald* (online ed, Auckland,15 August 2014). This criticism occurred in the context of s 216A of the Crimes Act 1961 and s 14 of the Government Communications Security Bureau Act 2003, both of which define "private communication" in a similar way to the Search and Surveillance Act.

[11] Search and Surveillance Act, s 3 (definition of "private communication").

[12] *Moreton v Police*, above n 4, at [22].

engage in drug dealing activities (or possibly other organised criminal activity) should now reasonably expect that their communications may be intercepted.[13]

4.15 The Law Commission previously discussed this issue in its 2010 Report, *Invasion of Privacy: Penalties and Remedies*. Considering the scope of the interception offence in the Crimes Act, the Commission concluded "[t]he likelihood of a privacy encroachment (through interception) should not be determinative of the application of the privacy protection provided by the interception offence".[14]

Communications that are not private

4.16 In *Moreton v Police*, William Young J also referred to the gap created by the fact that the warrant regime (that was in existence in 2002) only applied to "private" communications. While the interception of non-private communications is not an offence, it will often be difficult to carry it out lawfully – for instance, because entry on private property may be required to install the interception device. However, there is no ability to obtain a warrant for this, so enforcement agencies may be unable to do it at all.

4.17 His Honour noted this had led to an odd position where defendants would challenge the validity of a warrant on the basis that the communications intercepted were *not* "private". Police had to argue that a communication *was* private in order to sustain a warrant. William Young J stated:[15]

> It does seem strange and, indeed, contrary to common sense, that legislation should provide for interception of "private" communications but not for interception of communications which are not "private". One would think that privacy considerations would apply more strongly in relation to communications which are in the former category.

4.18 That analysis seems correct. The fact that the Act does not provide any authorisation framework for the interception of "non-private" communications means that they are paradoxically afforded greater protection from invasion by the State than "private" communications.

---

13 *Moreton v Police*, above n 4, at [24]–[28].

14 Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at [3.66].

15 *Moreton v Police*, above n 4, at [29].

Communications between machines

4.19 Another example of a type of communication unlikely to be covered by the definition of "private communication" is metadata or machine-to-machine communications. In broad terms, metadata is information about electronic activity that does not relate to its content. It includes the data created when forms of electronic communication are made, such as the time and date of a phone call or email, the email addresses or phone numbers of the parties, and the cell towers or IP addresses the communication was sent to and received from. It can also include websites visited by an Internet user.

4.20 Metadata can reveal information about relationships, location, identity and activity, which may be a valuable investigative tool. For example, metadata may allow Police to establish that a suspect is in communication with members of a criminal organisation, or has been visiting websites displaying objectionable material.

4.21 However, it does not appear to fit within the definition of "private communication". This is because the definition refers to the parties to the communication and their intentions, which implies that the communication must be between two or more people.

4.22 If that is the case, it arguably leaves a gap in the current law. It would mean the Act does not generally require or permit the issue of warrants to intercept metadata. But such interception may well breach section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA), meaning that enforcement agencies cannot do it without risking exclusion of the evidence in any criminal proceedings. It could also involve other breaches of the law, such as trespass, in order to install an interception device.

4.23 Currently, the Act deals with this difficulty in a limited way. Section 55(3)(g) requires a surveillance device warrant to permit an enforcement officer who obtains the content of a telecommunication under the warrant to direct the relevant network operator to provide call associated data related to the communication.[16] "Call associated data" is a class of data associated with telecommunications, covering the phone numbers involved and the time and duration of the call.[17]

4.24 However, the Act does not state whether this provision permits "interception" of call associated data in real-time or only production of the stored data after-the-fact. In

---

[16] Search and Surveillance Act 2012, s 55(3)(g).

[17] Telecommunications (Interception Capability and Security) Act 2013, s 3 (definition of "call associated data").

addition, and more significantly, it only covers a limited class of metadata associated with telecommunications. As noted above, there are other types of metadata that might be useful to investigations, such as metadata associated with Internet use.

4.25 Given that Police can legitimately intercept the content of private communications with a warrant, it seems logical that they should be able to obtain authorisation to intercept metadata. While some metadata can reveal a significant amount of private information about a person, few would argue that it should receive a greater level of protection than the content of private communications.

The scope of interception regimes in comparable jurisdictions

Canada

4.26 The Canadian interception regime is the most similar to ours. The Criminal Code makes it an offence to intercept a private communication using a device.[18] A communication is "private" if it is "made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it".[19]

4.27 The Criminal Code allows a judge to authorise the interception of private communications in limited circumstances. In general, a judge may only grant an interception warrant if he or she is satisfied that other investigative procedures have been tried and failed, are unlikely to succeed, or are not practicable given the urgency of the case.[20] Alternatively, there is a separate provision allowing an interception warrant to be issued where one of the parties to the communication consents to the interception.[21]

4.28 The Canadian definition of "private communication" is similar to the second limb of our Act's definition, in that it relies on reasonable expectations. It is therefore likely to give rise to the same problems that have been discussed above. However, the scope of the definition is likely to be less of an issue in Canada. As we have discussed in Chapter 2, the Canadian regime includes "general warrants" that can be issued in

---

18 Criminal Code RSC 1985 c C-46, s 184(1).

19 Section 183 (definition of "private communication").

20 Section 186(1).

21 Section 184.2.

relation to any activity not covered by a specific warrant provision. There is also a specific warrant regime for using devices or computer programs to obtain or record "transmission data", which is essentially metadata relating to telecommunications.[22]

United Kingdom

4.29 Under the Regulation of Investigatory Powers Act 2000 (UK) it is an offence to intercept any communications in the course of transmission by a public postal or telecommunications service.[23] There is a corresponding power for the Secretary of State to issue interception warrants to law enforcement and intelligence agencies.[24] The offence and the warrant provisions are not limited to interception using a "device" or to "private" communications. Interception of communications broadcast for general reception is recognised as an exception to the offence.[25]

4.30 In addition to the interception warrant provisions, there is a specific regime for access to "communications data". This includes metadata associated with postal communications and telecommunications, as well as other information held by a service provider about a customer.[26] Access to communications data can be authorised internally by a "designated person" within a law enforcement agency, and on broader grounds than interception warrants.[27] Communications data can also be accessed under an interception warrant where it is related to the communications being intercepted.[28]

Australia

4.31 Australian federal legislation prohibits the interception of any communications passing over a telecommunications system.[29] "Communication" is broadly defined as including any part of a conversation or message, whether in audio, visual, data, text, signals or any other form.[30] A judge or Administrative Appeals Tribunal member may

---

22 Section 492.2.

23 Regulation of Investigatory Powers Act 2000 (UK), s 1.

24 Section 5.

25 Section 2(3).

26 Section 21(4).

27 Section 22.

28 Section 5(6)(b).

29 Telecommunications (Interception and Access) Act 1979 (Cth), s 7.

30 Section 5 (definition of "communication").

issue a warrant permitting the interception of communications made via particular telecommunications services or devices.[31]

4.32 The use of listening devices is governed by separate legislation. There are State laws prohibiting the use of listening devices to record or listen to "private conversations".[32] These contain varying definitions of "private conversations", but the definitions are generally similar in effect to the definition of "private communication" in the Search and Surveillance Act.

4.33 The Surveillance Devices Act 2004 (Cth) as well as the various State Acts provide for the issue of warrants permitting the use of listening devices.[33] Unlike the interception offences, the issue of listening device warrants is not restricted to "private conversations". This avoids the problems created in New Zealand by the incorporation of the Crimes Act's reference to "private communications" into the warrant provisions.

Should the warrant regime apply to a wider range of interception activity?

4.34 Expanding the warrant regime to cover interception of communications and metadata more broadly would:

- increase certainty for enforcement agencies by providing a clear lawful basis for all interception, including of metadata; and
- increase transparency and proactive protection of privacy rights by expressly requiring authorisation to carry out any interception.

4.35 One possible approach would be to require a warrant for any interception of communications, except where consent is obtained or where the communication is made publicly available (such as a radio broadcast). "Communication" is not currently

---

31 Telecommunications (Interception and Access) Act 1979 (Cth), ss 46 and 46A.

32 Surveillance Devices Act 2007 (NSW), Listening Devices Act 1992 (ACT), Surveillance Devices Act 2007 (NT), Invasion of Privacy Act 1974 (Qld), Listening and Surveillance Devices Act 1972 (SA), Listening Devices Act 1991 (Tas), Surveillance Devices Act 1999 (Vic), Surveillance Devices Act 1998 (WA).

33 Surveillance Devices Act 2004 (Cth), ss 16–18. "Listening device" is defined as "any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation" (excluding hearing aids) (s 6).

defined in the Act, but the definition in the Government Communications Security Bureau Act 2003 provides a possible model:[34]

> **communication** includes signs, signals, impulses, writing, images, sounds, information, or data that a person or machine produces, sends, receives, processes, or holds in any medium

4.36 This definition is broadly framed and would cover the interception of metadata.

4.37 Such an approach would be broadly consistent with the overseas approaches discussed above, which do not limit the issuing of interception warrants to specific types of communications.[35]

4.38 An alternative approach would be to amend the definition of "private communication" to capture metadata and any other specific gaps identified. However, this would not resolve the apparent circularity of the definition. It is also unlikely to be a long-term solution, as further developments in technology are likely to result in the creation of new types of communications that may not be captured by the definition.

Q12 Should a surveillance device warrant be required to intercept all types of communications, rather than only "private" communications? If so, what specific exceptions to that requirement would be appropriate (for example, for publicly broadcasted communications)?

Q13 If the Act continues to require a warrant to intercept "private" communications only, should the definition of "private communication" be amended? If so, how?

The consent exception

4.39 As noted above, there is an exception to the general requirement to obtain an interception warrant where one of the parties to an oral communication consents to the interception. This exception means, for example, that a warrant is not required for Police to tape a conversation between an informant or undercover officer and a suspect.

4.40 Participant recording or interception with one party's consent is, however, a search for the purposes of NZBORA.[36] The admissibility of such recordings as evidence may be challenged on the basis that they were obtained unreasonably or unfairly. Whether such a challenge is upheld will depend on the circumstances. For instance, consent

---

34 Government Communications Security Bureau Act 2003, s 4 (definition of "communication").

35 Although the interception warrant regime is limited in this way in Canada, the existence of the general warrant regime means authorisation could likely be sought for other types of interception as well.

36 *R v A* [1994] 1 NZLR 429 (CA).

recordings have been excluded where an undercover officer or an informant who was acting as an agent of the State actively elicited a confession.[37]

4.41 The Act does *permit* (but not require) warrant applications for interception with consent, so this option is available to enforcement officers if they are unsure whether the intended interception will be reasonable.[38]

The approach taken to consent in comparable jurisdictions

4.42 Varied approaches are taken to interception with consent in comparable jurisdictions. In Australia, it is lawful for a law enforcement officer to use a listening device to record a communication in which he or she is involved, or where one party to the communication consents.[39] There is also provision for a police officer to intercept a telecommunication without a warrant where they are a party to it or the recipient of the telecommunication consents, but only in limited situations of threat to life or safety.[40]

4.43 In Canada, interception with the consent of one party is recognised as an exception to the interception offence.[41] However, in *R v Duarte* the Supreme Court of Canada held that warrantless interception with the consent of one party still violated section 8 of the Canadian Charter of Rights and Freedoms 1982 (the equivalent of section 21 of the NZBORA).[42] As a result, the Criminal Code was amended to provide for the issuing of judicial warrants to intercept private communications where one party consents.[43]

4.44 Similarly, in the United Kingdom the consent exception to the interception offence is only engaged where both the originator and the recipient of the communication consent.[44] If only one party consents to the interception, a warrant is still required.[45]

---

37 See the discussion in *K (CA106/2013) v R* [2013] NZCA 430 at [7]–[21] and [28]; and *R v Kumar* [2015] NZSC 124, [2016] NZLR 204 at [68]–[70].

38 Search and Surveillance Act 2012, s 47(2).

39 Surveillance Devices Act 2004 (Cth), s 38.

40 Telecommunications (Interception and Access) Act 1979 (Cth), s 7(4)–(5).

41 Criminal Code RSC 1985 c C-46, s 184(2)(a).

42 *R v Duarte* [1990] 1 SCR 30.

43 Criminal Code RSC 1985 c C-46, s 184.2.

44 Regulation of Investigatory Powers Act 2000 (UK), s 3(1).

45 Section 3(2).

Does the consent of one party justify warrantless interception?

4.45 Like the definition of "private communication", the consent exception to the warrant requirement was carried through from the Crimes Act with little discussion in the Law Commission's 2007 Report.[46] There is an argument that the exception in its current form is inconsistent with the underlying basis of the Act – that any activity invading a reasonable expectation of privacy should generally be carried out pursuant to a warrant.[47]

4.46 The rationale behind permitting interception with one party's consent is that it is equivalent to that party recalling the conversation and giving evidence as to what occurred.[48] The interception simply provides a more accurate record.

4.47 But the consent of one party to a communication does not necessarily lessen the reasonable expectations of privacy of the other party or parties. The Canadian courts have accepted there is a fundamental difference between a member of the public recording a conversation they are involved in of their own volition and an interception by the State.[49] No law can guarantee a communication will not be repeated by those who are party to it. But part of the role of the State is to protect human rights, including the right to be free from unreasonable search and seizure. Arguably, this means State agencies should generally be required to satisfy an independent issuing officer before intercepting private communications.

4.48 Requiring a warrant for interception with the consent of only one party would ensure that the assessment of what is reasonable or unreasonable in the circumstances is made by an independent issuing officer rather than enforcement officers. It would also allow the issuing officer to impose any appropriate conditions on how the interception is carried out. Ultimately, it would increase protection for privacy rights and help to ensure the admissibility of the evidence in subsequent proceedings.

4.49 On the other hand, requiring enforcement agencies to obtain a warrant in such situations may place a high administrative burden on those agencies. It may interfere

---

46 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.76].

47 See Cabinet Business Committee "Law Commission Report Search and Surveillance Powers: Paper 2: Interception and Surveillance" (14 March 2008) CBC (08) 85 at [47]; Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.131].

48 See *R v A*, above n 36, at 434, 437, 438 and 448–449.

49 See *R v Duarte*, above n 42, at 42–49.

with standard practices, as the consent exception is relied on frequently in the everyday activities of enforcement agencies. For example, it provides a basis for phone calls to enforcement agencies to be recorded as a matter of course.

4.50 An alternative to requiring a warrant for all consent interception would be to limit the warrant requirement to where:

- the consenting party is an enforcement officer or an agent of the State; and
- the non-consenting party or parties are unaware of the consenting party's true identity or the fact that they are an agent of the State.

4.51 "Agent of the State" is a term used in case law to refer to a person who is acting at the direction of the State (that is, they would not have engaged with the suspect at all or in the same manner but for an enforcement agency's influence).[50]

4.52 This approach would allow enforcement agencies to intercept a communication without a warrant at the request of a person: for example, where the person has been receiving abusive phone calls. It would also ensure that enforcement officers could still record conversations they have with members of the public who are aware they are speaking to an enforcement officer – in which case they arguably cannot expect the communication to remain private. However, a warrant would be required in order to carry out interception in the context of undercover activity.

If the consent exception is retained, should it be broader in scope?

4.53 Currently, the consent exception only applies to covert audio interception of oral communications, even though the unlawful interception offence in the Crimes Act is not limited in this way. We understand that this creates some difficulties. For example, it means Police cannot intercept text messages being sent to a person who requests the interception.

4.54 In principle, we see no reason for distinguishing between oral communications and other forms of communication. In the event that the consent exception is retained in some form, it could be amended to cover any type of communication. This would be more consistent with the approach taken to determine whether interception without a warrant is justified.

---

[50] See *K (CA106/2013) v R*, above n 37, at [21].

Q14 Should the Act be amended to require a warrant to intercept oral communications where only one party to the communications consents?

Q15 If the consent exception is retained, should it be amended to:

(a) Apply in more limited circumstances (for example, not where the consenting party is an undercover officer)?

(b) Apply to any type of communication (such as emails), not just oral communications?

TRACKING DEVICE WARRANTS

The current law

4.55 The Act requires enforcement officers to obtain a surveillance device warrant in order to use a tracking device, except where it is:[51]

> …installed solely for the purpose of ascertaining whether a thing has been opened, tampered with, or in some other way dealt with, and the installation of the device does not involve trespass to land or trespass to goods …

4.56 "Tracking device" is defined in section 3:[52]

> **tracking device—**
>
> (a) means a device that may be used to help ascertain, by electronic or other means, either or both of the following:
>
> (i) the location of a thing or a person:
>
> (ii) whether a thing has been opened, tampered with, or in some other way dealt with; but
>
> (b) does not include a vehicle or other means of transport, such as a boat or helicopter

4.57 There is no exception to the requirement to obtain a tracking device where the person being tracked (or the person entitled to possession of the thing being tracked) consents.

The scope of the tracking regime

4.58 We understand enforcement agencies have encountered difficulties as a result of the broad definition of "tracking device". The definition appears to capture a range of activities that are either not focused on the investigation of crime and/or are carried out with consent.

4.59 This does not simply create an administrative burden by requiring enforcement officers to obtain a warrant. It creates additional problems because—although the Act requires a warrant to be obtained for any use of a tracking device—a warrant is

---

51 Search and Surveillance Act 2012, s 46(1)(b).

52 Section 3 (definition of "tracking device").

unlikely to be available where the tracking is for a purpose other than the investigation of offending. A warrant can only be issued where there are reasonable grounds to believe an offence has been, is being or will be committed, and that the use of the device will obtain evidential material in relation to that offence.

Tracking with consent

4.60 There is no consent exception to the requirement to obtain a tracking device warrant. This means that the Act appears to require a warrant in order to:

- track vehicles or things belonging to the enforcement agency or enforcement officers (which agencies may wish to do for safety purposes or to locate stolen vehicles or items); or
- track stolen cell phones or other electronic devices at the request of their owner.

4.61 This seems counter-intuitive, as there is unlikely to be any invasion of privacy in such cases. We are therefore interested in submitters' views on whether a consent exception should be introduced.

Tracking for search and rescue purposes

4.62 The requirement to obtain a warrant to use tracking devices may also create an obstacle where there are serious concerns about a person's safety. For example, it may prevent Police from tracking the phone of a missing person as part of a search and rescue operation, or using the radar on a police launch to locate a boat when a distress signal has been sent out.

4.63 Allowing tracking to occur in cases such as this would appear to be consistent with the rationale behind section 14 of the Act, which allows constables to enter a place without a warrant where there is risk to the life or safety of any person that requires an emergency response. We also note that the Privacy Act 1993 recognises risks to the life or health of any person as a legitimate reason for disclosing personal information.[53]

Use of radar for monitoring purposes

4.64 The definition of "tracking device" may also capture the use of radar technology, as it discloses the location of a thing. Radar is used to scan an area for the presence of ships

---

[53] Privacy Act 1993, s 6, principle 11(f).

or aircraft and shows where they are located. For example, ships and aircraft have on-board radars to ensure they do not collide with other vessels.

4.65 Where radar is used by an enforcement agency to track a specific known vessel for the purpose of investigating a suspected offence, a surveillance device warrant can be sought. However, radar can also be used for general monitoring and inspection purposes. For example, fisheries officers may wish to use radar to help them locate vessels for the purposes of carrying out their statutory powers of inspection to ensure compliance with the Fisheries Act 1996.[54] The criteria for obtaining a warrant would not be met in these types of cases. In addition, a warrant regime is unlikely to be appropriate given the necessarily ongoing nature of inspection and monitoring activities.

4.66 In most instances the radar technology used by enforcement agencies does not provide information about the identity of a specific vessel or person; it simply indicates that some type of vessel is present. In this sense it may be comparable to flying an aircraft over an area and sighting vessels, or observing the location of various people in a public space.

4.67 Arguably, using radar in this way does not involve a significant invasion of privacy because it only discloses information about what is occurring in public spaces and does not identify individuals. In addition, given that radars are present on most ships and aircraft, persons operating vessels are likely to expect that the location of the vessel will be known to others.

Q16 Should the Act permit certain types of tracking activity without a warrant (for example, tracking with consent or in search and rescue situations, or using radar for monitoring purposes)?

[54] See s 199 of the Fisheries Act 1996, which permits fisheries officers to stop and board vessels for inspection purposes.