Chapter 3 – Surveillance: Availability of surveillance device warrants

INTRODUCTION

3.1 This chapter considers the availability of surveillance device warrants under the Search and Surveillance Act 2012 (the Act), including whether the requirements around authorisation of surveillance are set at the right level and whether the regime governs a wide enough range of techniques.

3.2 Currently the Act treats surveillance as inherently more intrusive than searches and imposes greater controls on its use. However, the Act only regulates the use of a limited class of surveillance devices. It says nothing about the extent to which other surveillance techniques can be used.

3.3 Technology has developed significantly since the Act was originally drafted in 2007. As we have noted in the previous chapter, our preliminary discussions with enforcement agencies suggest there is some uncertainty at an operational level about the extent to which new technology or novel techniques can be used. In addition, the wide availability and use of technology by the government, private sector and individuals raises a question about whether there is still justification for having stronger restrictions on the use of surveillance devices compared to other types of searches.

3.4 In the discussion that follows, we discuss whether the Act should:

- continue to treat surveillance (or at least certain types of surveillance) as more intrusive than searches; and/or
- explicitly address the use by enforcement agencies of other types of surveillance not currently referred to in the Act.

OVERVIEW OF THE SURVEILLANCE DEVICE WARRANT REGIME

Before the Search and Surveillance Act

3.5 Prior to 2012 there was no general regime in legislation dealing with surveillance for law enforcement purposes. Surveillance involving trespass to land or goods was generally unlawful, while non-trespassory surveillance could breach section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA). The search warrant regime then contained in section 198 of the Summary Proceedings Act 1957 could not authorise

surveillance, because it did not allow for anticipatory or prospective warrants.[1] However, some specific criminal offences relating to interception and visual recordings recognised exceptions for law enforcement purposes.[2] In addition, the Summary Proceedings Act included a regime for issuing tracking device warrants.[3]

3.6 The Law Commission's 2007 Report, *Search and Surveillance Powers*, recommended introducing a single statutory scheme governing the use of audio, visual and tracking devices by enforcement officers.[4] This scheme would be as consistent as possible with that applying to searches. The Commission also recommended the introduction of a residual warrant regime that would apply to other types of surveillance devices not explicitly covered by the surveillance device warrant regime. These recommendations were accepted (but, as we discussed in Chapter 2, the residual warrant regime was amended during the passage of the Bill to become the declaratory order regime[5]).

The current regime

3.7 The Act requires enforcement officers to obtain a surveillance device warrant in order to:[6]

- use an interception device to intercept a private communication;
- use a tracking device (unless no trespass is involved and the purpose is solely to detect whether a thing has been opened, tampered or otherwise dealt with);
- use a surveillance device in a manner involving trespass to land or goods; or
- use a visual surveillance device to:
    - observe and/or record private activity in private premises; or

---

1 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [6], [145]–[146], [150] and [210]–[212].

2 Section 216B of the Crimes Act 1961 makes it an offence to intercept a private communication with an interception device. Prior to the Search and Surveillance Act 2012, the Crimes Act permitted High Court judges to issue warrants authorising Police to intercept private communications in relation to a limited class of offences where strict criteria were met: Crimes Act 1961, Part 11A and Misuse of Drugs Amendment Act 1978, ss 14–29 (all now repealed). Under section 216H of the Crimes Act it is an offence to make an intimate visual recording of a person without their consent. Constables and certain other persons are exempt from liability if they are carrying out functions relating to the prevention, detection, investigation, prosecution or punishment of offences, or security or safety: Crimes Act 1961, s 216N.

3 Summary Proceedings Act 1957, ss 200A–200P (now repealed).

4 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at 328–330 and recommendations 11.3 and 11.5.

5 See at paragraphs [2.30]–[2.41] above.

6 Search and Surveillance Act 2012, s 46.

- observe and/or record private activity in the curtilage of private premises if the observation exceeds three hours in a 24-hour period or eight hours in total (for the purposes of a single investigation or connected series of investigations).

3.8 A "surveillance device" means an interception device, tracking device or visual surveillance device.[7] As discussed in Chapter 2, enforcement officers are not expressly required to obtain warrants to carry out surveillance using other types of devices.

3.9 A judge may issue a surveillance device warrant if he or she is satisfied there are reasonable grounds to suspect that a relevant offence has been, is being or will be committed, and to believe that the use of the device will obtain evidential material in respect of the offence.[8]

3.10 The Act does recognise some exceptions to the requirement to obtain a surveillance device warrant. An enforcement officer does not require such a warrant to:[9]

- record what he or she observes while lawfully on private premises;
- make a covert audio recording of a voluntary oral communication between two or more persons, with the consent of at least one of them; or
- carry out activities authorised under another enactment (including interception warrants issued under the New Zealand Security Intelligence Service Act 1969 or Government Communications Security Bureau Act 2003.

3.11 The Act also permits enforcement officers to use a surveillance device without a warrant for up to 48 hours in some situations of emergency or urgency.[10] This warrantless power only applies in relation to certain classes of offences and where it is impracticable to obtain a warrant within the time available.

3.12 An enforcement officer who carries out urgent warrantless surveillance must, however, report to a judge within one month about the circumstances in which the device was used and the results of the surveillance.[11] The judge may make directions

---

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

8 Section 51. As discussed further below, relevant offences are those in respect of which a search warrant could be applied for under the Act or any enactment in the Schedule.

9 Section 47(1).

10 Section 48.

11 Section 60.

about the retention or destruction of the material obtained, report any unauthorised use of a surveillance device to the chief executive of the relevant agency or order that the subject of the surveillance be notified.[12]

How has the surveillance device warrant regime operated in practice?

3.13 Between 18 April 2012 (when the surveillance device warrant provisions came into force) and the 2014/15 reporting year, a total of 351 applications for surveillance device warrants were made by Police.[13] All of those applications were granted. The number of warrants has increased each year, with 122 being issued in 2014/15. The largest number of warrants related to interception, but the use of tracking and visual surveillance devices was almost as frequent.

3.14 Each year the number of people charged in criminal proceedings in partial reliance on evidential material obtained under a surveillance device warrant exceeded the number of such warrants issued. It can be inferred from this that most warrants resulted in evidential material being successfully obtained (sometimes in relation to offending by multiple people), which suggests applications on the whole are being accurately assessed. We were shown some examples of surveillance device warrant applications by Police and they appeared to provide the issuing officer with a significant level of detail on which to base his or her decision.

3.15 We are aware of some discrete issues with the operation of the surveillance device warrant regime in particular contexts, which have been raised with us by enforcement agencies or identified in case law. We discuss those issues in Chapters 4 and 5.

3.16 Those discrete issues aside, our overall impression from speaking to enforcement agencies and surveying issuing officers is that the surveillance device warrant regime has largely operated effectively in respect of those devices it applies to. That is consistent with our review of the case law since the Act came into force, which did not

---

12 Search and Surveillance Act 2012, s 62.

13 New Zealand Police *Annual Report 2012/13* at 109 and *Annual Report 2014/15* at 143. We note that, as discussed above, other enforcement agencies can obtain some types of surveillance device warrants, so this does not provide a full picture of all the warrants applied for and obtained.

raise any major issues with the operation of the surveillance device warrant provisions.[14]

3.17 For that reason, our discussion in this chapter focuses on whether there are any gaps in the availability of surveillance device warrants that need to be addressed.

THE RELATIONSHIP BETWEEN SURVEILLANCE AND SEARCH

As discussed in the 2007 Law Commission Report

3.18 As a general proposition, the Law Commission's 2007 Report proceeded on the basis that surveillance device warrants should be available in the same circumstances as search warrants. The Commission said:[15]

> …surveillance device warrants ought to be available on the same basis as search warrants. The former are not intrinsically more intrusive than the latter; that depends entirely on their scope and manner of execution in the individual case. In circumstances where the exercise of coercive powers for the investigation of offending is justified, therefore, enforcement agencies should have the ability to apply for the type of warrant that will obtain the evidential material being sought most efficiently and effectively.

3.19 In line with that reasoning, the Commission recommended that surveillance device warrants should be available:

- in relation to any offence for which a search warrant could be issued;[16] and
- in relation to any agency that has a search warrant power for law enforcement purposes.[17]

3.20 However, the Commission did recommend that surveillance device warrants should only be issued by judges rather than all issuing officers.[18] This point was finely balanced. The Commission recognised that it made little sense to split authority for issuing different types of warrants, given that one form of intrusion on reasonable expectations of privacy was not necessarily more intrusive than others.[19] But since surveillance devices were an area of particular public concern, on balance it

---

14 The only case we are aware of that raises a potential issue with the operation of the surveillance device warrant provisions is *Murray v R* [2016] NZCA 221. That case considered the manner in which intercepted phone calls are monitored by Police, an issue that we address at paragraphs [5.16]–[5.28] below.

15 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.79]. See also at [11.82].

16 Recommendation 11.8.

17 Recommendation 11.9.

18 Recommendation 11.17.

19 At [11.100].

recommended retaining the status quo in the existing interception and tracking device regimes (which required judicial approval).[20]

As recognised in the Search and Surveillance Bill

3.21 These recommendations were reflected in the Search and Surveillance Bill as introduced. However, the Bill was significantly redrafted in line with recommendations made by the Select Committee. These changes included restricting the use of audio surveillance and visual trespass surveillance to specified offences and agencies (discussed further below).

3.22 The Select Committee's recommendations were prompted by submitters' concerns that enforcement officers would receive new surveillance powers that would be disproportionate to the offending likely to be investigated.[21] Contrary to the view of the Law Commission, the Select Committee considered that some types of surveillance (namely audio surveillance and visual trespass surveillance) were inherently more intrusive than others and should be treated accordingly.[22]

As enacted in the Search and Surveillance Act

3.23 The conditions on applying for and issuing surveillance device warrants are similar to search warrants, aside from three key differences.

3.24 First, unlike search warrants, which can be issued by any issuing officer, all surveillance device warrants must be issued by a judge.[23]

3.25 The other two differences only apply to surveillance device warrants that permit visual surveillance involving trespass to land or goods, or the use of an interception device.[24] These types of warrants can only be issued:

- if they relate to offences punishable by at least seven years' imprisonment or other specified offences;[25] and
- on the application of a New Zealand Police constable.[26]

---

20 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.101].

21 Search and Surveillance Bill 2010 (45-2) (select committee report) at 3.

22 At 4.

23 Search and Surveillance Act 2012, s 53.

24 Sections 3 (definition of "trespass surveillance"), 45 and 49(5).

25 Section 45. The specified offences are under the Arms Act 1983 and Psychoactive Substances Act 2013.

3.26 These restrictions do not apply to the use of visual surveillance devices where no trespass is involved, or to the use of tracking devices. Warrants can be sought for these activities by any enforcement officer and in relation to any offence for which the applicant could apply for a search warrant.[27] For constables, this means any imprisonable offence.[28]

Comparable jurisdictions

United Kingdom

3.27 The United Kingdom in some respects takes the opposite approach to New Zealand. It appears that, at least in relation to police investigations, surveillance in the United Kingdom can be authorised in a wider range of circumstances than searches. This is because of the different tests that apply to determining when surveillance and search warrants may be issued. However, interception is restricted to a narrower class of agencies than searches and other types of surveillance.

3.28 Surveillance powers in the United Kingdom are primarily contained in the Regulation of Investigatory Powers Act 2000 (UK), while search powers are set out in the Police and Criminal Evidence Act 1984 (UK) (PACE).

3.29 Surveillance can be authorised if the proposed activity is necessary to prevent or detect serious crime[29] and proportionate to the outcome sought.[30] This language is relatively broad, in the sense that it does not require a connection to a specific offence or evidential material. Searches, by contrast, can only be authorised where there are reasonable grounds to believe that an indictable offence has been committed and that

---

[26] Search and Surveillance Act 2012, s 49(5)(a). There is provision in ss 49(5)(b) and 50 for the Department of Internal Affairs or New Zealand Customs Service to be authorised to carry out these types of surveillance through an Order in Council, but we understand this has not occurred to date.

[27] Search and Surveillance Act 2012, s 51(a)(i).

[28] Search and Surveillance Act 2012, s 6(a). The offences that non-Police enforcement officers can seek search warrants for differ depending on the legislation that confers their search powers.

[29] "Serious crime" is an offence that could reasonably be expected to result in a sentence of imprisonment for three years or more, or that involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose (Regulation of Investigatory Powers Act 2000 (UK), s 81(2) and (3)).

[30] Regulation of Investigatory Powers Act 2000 (UK), ss 5, 28, 29 and 32.

there is material on the premises that is likely to be of substantial value to the investigation of that offence.[31]

3.30 Surveillance is authorised by the Secretary of State, in the case of interception,[32] or by officials of various levels for other types of surveillance.[33] Interception warrants can only be applied for by Police, intelligence agencies and the New Zealand Customs Service,[34] while other types of surveillance warrants are available to a wider range of government agencies.[35] Searches are authorised by justices of the peace.[36] Search warrants under PACE are only available on application by a constable,[37] but various other pieces of legislation confer search powers on additional agencies.[38]

Australia

3.31 The position in Australia appears to be similar to that in New Zealand. Surveillance must be authorised by judges, relate to more serious offences than searches (although the threshold is lower than in New Zealand) and be carried out by a more limited class of enforcement agencies.

3.32 Surveillance device warrants are governed at the federal level by the Surveillance Devices Act 2004 (Cth). They can be issued by an eligible judge or nominated member of the Administrative Appeals Tribunal.[39] Surveillance device warrants are available to Police and a limited class of other specified bodies (such as the Australian Commission for Law Enforcement Integrity, which investigates law enforcement-related corruption issues).[40] They can be issued in relation to offences punishable by three or more years' imprisonment.[41]

---

31 Police and Criminal Evidence Act 1984 (UK), s 8.

32 Regulation of Investigatory Powers Act 2000 (UK), s 7.

33 See below at paragraphs [3.86]–[3.89].

34 Regulation of Investigatory Powers Act 2000 (UK), s 6.

35 Section 30 and Schedule 1.

36 Police and Criminal Evidence Act 1984 (UK), s 8.

37 Section 8.

38 See for example the Customs and Excise Management Act 1979 (UK) and Sea Fisheries Act 1968 (UK).

39 Surveillance Devices Act 2004 (Cth), s 11.

40 Sections 6 and 14.

41 Sections 14 and 16.

3.33 Search warrants can be issued by authorised justices of the peace in addition to judges[42] and in relation to any offence.[43] Search warrants under the Crimes Act 1914 (Cth) can only be issued to constables.[44] However, as in the United Kingdom, there are specific search powers conferred on various other agencies in separate legislation.[45]

Canada

3.34 The Canadian legislation does not distinguish between searches and surveillance in terms of the range of offences. In addition, searches and most kinds of surveillance can be carried out by a broad range of agencies. However, the legislation does require surveillance warrants (other than tracking warrants) to be issued by judges and restricts the issue of interception warrants to "last resort" situations.

3.35 Warrants for searches, tracking or interception with the consent of one party to a communication can be issued to any public officer who is designated to enforce any Act.[46] Interception without consent can be carried out by any specified person, but the application must be signed by the Attorney-General, the Minister of Public Safety and Emergency Preparedness or a designated agent.[47]

3.36 As discussed in Chapter 2, other types of surveillance are captured by a general warrant regime. General warrants can be issued to "peace officers", which includes police officers and designated corrections, customs, immigration, fisheries and defence personnel.[48]

3.37 Warrants authorising searches[49] or tracking[50] can be issued by a justice of the peace, while interception warrants[51] and general warrants[52] must be issued by a judge.

---

42 Crimes Act 1914 (Cth), s 3C (definition of "issuing officer").

43 Sections 3C (definition of "evidential material") and 3E.

44 Crimes Act 1914 (Cth), ss 3C (definition of "executing officer") and 3F.

45 See for example the Taxation Administration Act 1953 (Cth).

46 Criminal Code RSC 1985 c C-46, ss 184.2(2), 487(1) and 492.1.

47 Section 185(1).

48 Sections 2 (definition of "peace officer") and 487.01(1).

49 Sections 2 (definition of "justice") and 487(1).

50 Section 492.1(1)–(2).

51 Sections 184.2(3) and 186(1).

52 Section 487.01.

3.38 All warrants under the Criminal Code can be issued in respect of any offence. However, there are some additional restrictions applying to warrants permitting interception without consent. These warrants can only be issued where other investigatory techniques have been tried and failed, are unlikely to succeed or are impracticable because the situation is urgent.[53]

Is surveillance inherently more intrusive than searching?

3.39 Search warrants can permit entry onto private premises, and the search and seizure of personal belongings, files and computers. These are inherently intrusive actions and may result in enforcement agencies being privy to information that individuals would expect to be private. However, search warrants are generally only exercised on a single occasion (or on multiple occasions but only to the extent specified in the warrant) and relate to information already in existence at that time.

3.40 Like searches, the nature of surveillance activity can be intrusive – for instance, where a private conversation is recorded or a video is taken inside a person's home. In addition, surveillance is inherently anticipatory. It may be ongoing for up to 60 days, so the intrusion on privacy can continue for a longer period than under a search warrant. This may allow an enforcement agency to amass a greater volume of information about a person than it could under a search warrant.

3.41 In addition, the anticipatory and ongoing nature of surveillance means it must be carried out covertly. Notice cannot be given at the time of the surveillance in the same way as it is at the time of a search, as this would alert the target and jeopardise the operation.

3.42 Despite its anticipatory nature, surveillance may not necessarily be more intrusive than searches in all cases. It might allow an enforcement agency to obtain the information required without physically entering a person's home and searching through their things. It also does not generally deprive a person of their belongings in the same way that physical seizure might (for example, during a search a computer may be seized to allow examination and copying).

3.43 Because of the amount of information that is now stored electronically, the information obtained under a surveillance device warrant is often similar to or the same as that which would be obtained under a search warrant. For example, the same

---

[53] Criminal Code RSC 1985 c C-46, s 186(1).

email or text communication might be obtained under an interception warrant, if it is intercepted while in transit, or under a search warrant, once it has been received and is stored on a computer, phone or remote server.

3.44 This creates an odd distinction. Enforcement agencies other than Police cannot get surveillance device warrants to intercept communications (as these can only be issued to constables).[54] However, they can wait until just after a communication has been received and then get a production order or search warrant to obtain it. One enforcement agency we spoke to said this causes difficulty for them in practice. When investigating certain types of offending (such as blackmarket trading online), they need to act quickly to disrupt the activity or obtain evidence. This is difficult to achieve without real-time access to communications.

3.45 Similarly, Police cannot get a warrant to intercept communications where the relevant offence is punishable by less than seven years' imprisonment,[55] but may be able to access the same communications after-the-fact through a production order directed to a telecommunications provider. This may inhibit their ability to respond quickly.

3.46 At a principled level, it is difficult to see why the threshold for accessing a communication should be different depending on the time at which it is accessed, unless one method of access is considered to be inherently more intrusive than the other.

3.47 We are interested in hearing views on whether the Act should allow all types of surveillance device warrants to be issued by any issuing officer, to any enforcement officer and/or in relation to the same offences as search warrants. This would allow issuing officers to assess, in cases where both search and surveillance are an option, which means of obtaining the evidential material sought is most appropriate. In doing so, they would weigh the likely effectiveness of the proposed approach against the extent of privacy invasion involved and consider whether there are less intrusive methods available. This could help to ensure that investigatory activities involve the lowest level of privacy intrusion possible in the circumstances.

3.48 On the other hand, such a change would also allow increased use of surveillance. If there are good reasons for concluding that surveillance (or at least certain types of

---

54 Search and Surveillance Act 2012, s 49(5)(a).

55 Section 45.

surveillance) is inherently more intrusive than searches, such a development may not be desirable.

3.49 We note for clarity that we do not suggest issuing officers other than judges should be able to approve residual warrants (discussed in Chapter 2), should they be adopted.

Q4 Should all surveillance device warrants be available in respect of the same offences as search warrants (that is, any imprisonable offence)?

Q5 Should all surveillance device warrants be available to any enforcement officer who can apply for a search warrant?

Q6 Should the power to issue surveillance device warrants be extended to all issuing officers (rather than just judges, as is currently the case)?

Warrantless search powers

3.50 As noted above, under the current regime a surveillance device warrant can only be issued if the suspected offence is one in respect of which the enforcement officer could apply for a search warrant.[56] This approach was adopted from the Law Commission's 2007 Report. However, the Report did not expressly consider whether it was appropriate to allow surveillance device warrants to be issued to an enforcement officer who has a warrantless search power only.

3.51 The Act allows search warrants to be issued in respect of any imprisonable offence, but only constables are empowered to apply for them.[57] Non-Police enforcement officers can only apply for search warrants if they are expressly permitted to do so under their own governing legislation.

3.52 Some pieces of legislation listed in the Act's Schedule contain specific provisions allowing search warrants to be issued.[58] Others confer warrantless powers on non-Police enforcement officers but do not enable applications for search warrants. For example, park rangers have warrantless powers to search certain vehicles and structures in national parks for evidence of offending,[59] but they have no corresponding ability to apply for a search warrant.

---

56 Search and Surveillance Act 2012, s 51(a)(i).

57 Section 6(a).

58 See for example s 293A of the Immigration Act 2009.

59 National Parks Act 1980, s 65(1).

3.53 Currently, those enforcement officers with warrantless powers but no ability to obtain search warrants cannot obtain surveillance device warrants. So, for instance, a park ranger can enter and search a boat without a warrant, but cannot obtain a surveillance device warrant to track the movements of a boat that he or she has reason to believe will be used to commit an offence (such as removing protected objects[60] or entering a specially protected area[61]). Some non-Police enforcement agencies told us that this causes difficulty for them, as it prevents them from using the most effective investigation tools for a particular context.

3.54 A non-Police enforcement officer could ask Police to apply for a surveillance device warrant on their behalf, since constables can apply for a search warrant in respect of any imprisonable offence. However, the investigating officer is likely to be in the best position to submit a comprehensive warrant application. A constable applying on their behalf would need to be brought up to speed with all of the information supporting the application, which is unlikely to be an efficient use of time.

3.55 Warrantless search powers are only granted where there is some exceptional reason why a warrant should not be required in a particular circumstance (for example, because of urgency).[62] This means that warrantless powers require higher justification than search warrant powers. Where Parliament has decided there is sufficient justification for conferring a warrantless power on a class of enforcement officers, it seems logical to extend to them the same ability to apply for surveillance device warrants as is available to enforcement officers with search warrant powers.

Q7 Should surveillance device warrants be able to be issued where the enforcement officer has a warrantless power of search in relation to the suspected offence?

WHAT TYPES OF SURVEILLANCE SHOULD THE ACT COVER?

3.56 The surveillance device warrant regime in the Act only covers the use of certain types of devices for specific purposes.[63] As discussed in Chapter 2, the use of other devices or techniques was originally intended to be authorised under a residual warrant

---

60 National Parks Act 1980, s 60(1)(d).

61 Section 13(5)(a).

62 See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.4]; Cabinet Business Committee "Law Commission Report Search and Surveillance Powers: Paper 4: Warrantless Powers" (14 March 2008) CBC (08) 87 at [4]; *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014), guideline 18.2.

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

regime. However, that regime was replaced with declaratory orders, which cannot authorise anything that involves trespass or might breach section 21 of NZBORA.[64] As a result, the Act simply does not deal with the legality or otherwise of surveillance falling outside the surveillance device warrant regime.

3.57 Enforcement agencies told us this causes uncertainty for them and prevents them from using techniques not explicitly covered by the Act. It may also be problematic from a transparency perspective, as the scope of enforcement agencies' powers is not clear on the face of the Act.

3.58 In Chapter 2, we suggested some possible ways to address this issue. A residual warrant regime could be introduced, and/or the types of surveillance for which a warrant can (or must) be obtained could be revised.

3.59 In this section we discuss some of the specific types of surveillance that are not currently captured by the surveillance device warrant regime and ask whether and how they should be dealt with by the Act. The answer to the "how" question will depend in part on whether a residual warrant regime is introduced. If it is, regulating the types of surveillance discussed below may simply be a matter of ensuring that the residual warrant regime is sufficiently broad to cover them. However, there would still be scope to provide for a different type of authorisation for specific kinds of surveillance (such as an internal authorisation or warrantless power). If no residual warrant regime is introduced, the Act may need to be more specific about what kinds of surveillance can be carried out and what type of authorisation is required.

Electronic surveillance

3.60 The limited scope of the surveillance device warrant regime means it does not cover some types of electronic surveillance. That is because either the device used is not expressly referred to in the Act or because the surveillance does not involve a device.

Devices not covered by the Act

3.61 The surveillance device warrant regime only captures the use of visual surveillance devices, interception devices and tracking devices. There are other types of devices that might be used to monitor people, places or things. For example, thermal imaging

---

64 Search and Surveillance Act 2012, s 65.

devices can identify heat patterns in a building, and chemical residue detectors can screen for the presence of drugs in people's pockets or luggage.

3.62 Another class of device not covered is what is referred to in Australian legislation as a "data surveillance device". Like our Act, the Australian Surveillance Devices Act 2004 (Cth) contains a regime for authorising the use of specific types of surveillance devices. In most respects its scope is similar to the regime in our Act. However, it also provides for the issuing of warrants for "data surveillance devices", which are 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".[65]

3.63 This is likely to include, for example, devices or software that monitor the keys struck on the keyboard of a computer, take screenshots of a computer's screen or record search engine queries and websites visited.

3.64 Some of these functions could possibly be classed as visual surveillance (such as screenshots) or interception of private communications (such as emails or private messages). However, other types of data surveillance would not be covered by the surveillance device warrant regime in the Act.

3.65 For example, under the Act an interception is only captured if it relates to a "private" communication. As discussed further below, the definition of "private communication" is narrow and unlikely to cover the interception of data such as web browsing history or search engine queries. It is also unlikely to capture the use of devices such as International Mobile Subscriber Identity (IMSI) catchers or grabbers, which mimic cell towers and intercept non-content data from mobile phones (such as the IMSI number[66] of a phone, which can be used to identify its owner).

Surveillance without devices

3.66 Unlike the Australian definition of "data surveillance device", the Act does not appear to cover the use of surveillance programs or software. "Device" is not defined in the Act, but the definitions of "interception device" and "visual surveillance device" both refer to an "instrument, apparatus, equipment, or other device".[67] This implies that

---

65 Surveillance Devices Act 2004 (Cth), s 6.

66 An International Mobile Subscriber Identity (IMSI) number is located in the SIM card and identifies the subscriber.

67 Search and Surveillance Act 2012, s 3.

"device" is intended to carry its ordinary meaning of a tangible thing, rather than an intangible thing such as a computer program.

3.67 Electronic surveillance can increasingly be carried out using techniques that do not require a device. For example, software can be installed on a suspect's computer that will automatically send certain information back to the enforcement agency on a continuing basis. This would not appear to fit within the current surveillance device warrant regime, even though it might achieve the same effect as the use of an interception device.

3.68 In the United Kingdom, the interception offence and corresponding warrant powers are not limited to interception using a "device".[68] There are also other provisions applying to surveillance that does not involve the use of a device, such as section 93 of the Policing Act 1997 (UK), which allows a chief constable or commissioner to authorise interference with property or wireless telegraphy. This section has apparently been used to authorise the use of IMSI catchers, for example.[69] Surveillance that is likely to result in obtaining personal information about someone may also be caught by the "directed surveillance" regime, which is discussed below in relation to in-person surveillance.

3.69 In Canada, the definitions of "tracking device" and "transmission data recorder" explicitly include computer programs.[70]

Should the Act govern the use of a wider range of electronic surveillance?

3.70 The types of electronic surveillance discussed above could be considered by a court to invade a reasonable expectation of privacy in some circumstances. In the absence of a warrant, their use may breach section 21 of NZBORA. In addition, in some cases they may amount to a criminal offence. For instance, under section 252 of the Crimes Act 1961 it is an offence to access a computer system without authorisation.

3.71 Because of this, the fact that the Act does not provide an authorisation framework for these methods means that in many cases they simply cannot be used by enforcement agencies. In other cases, they may be used if enforcement agencies reach the view that

---

68 Regulation of Investigatory Powers Act 2000 (UK), ss 1 and 5.

69 See David Anderson QC *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) at [4.72].

70 Criminal Code RSC 1985 c C-46, ss 492.1(8) (definition of "tracking device") and 492.2(6) (definition of "transmission data recorder").

they will not breach section 21 of NZBORA in the particular circumstances, but the position lacks clarity.

3.72 At least some of the surveillance methods discussed above appear to be less intrusive than those already permitted under the Act. For example, the use of a thermal imaging device is unlikely to be considered as intrusive as intercepting a person's private communications or installing a video surveillance device on their property. The inability of enforcement agencies to use these less intrusive methods does not have any obvious principled basis. Rather, gaps in the Act's warrant regime seem to have arisen inadvertently as technology has developed in unanticipated ways.

3.73 Broadening the surveillance regime in the Act to both permit and control the use of a greater range of electronic surveillance methods would:

- make the warrant regime in the Act more coherent and rational by enabling the use of methods comparable to (or less intrusive than) those already authorised;
- allow enforcement agencies to use the most up-to-date, efficient and effective methods to access information to support their investigations; and
- place appropriate protections around the use of those methods, through the imposition of statutory criteria, authorisation by an appropriate person (which could vary depending on the activity involved) and the ability for that authorising person to place conditions around how the investigation is conducted.

Options for reform

3.74 There are two broad options for how the Act could be amended to cover a greater range of electronic surveillance activities. First, the surveillance device warrant provisions could be amended to specifically refer to an increased range of electronic surveillance. For example, the provisions could be extended to cover the use of:

- computer programs to access private communications and/or information generated by a person's computer or other device; and
- devices or other electronic means that can disclose information about activity occurring within private premises or things concealed on a person or in personal belongings.

3.75 That approach would, however, carry the risk of becoming outdated in the same way that the current surveillance device warrant regime has. There is potential for

technology to develop in ways that cannot yet be anticipated, and specifically extending the regime still may not capture these future developments.

3.76 The second approach would be to cover these types of surveillance through a more general regime focused on the type of information being accessed rather than the methods that are used to access it. The residual warrant regime discussed in Chapter 2 is an example of this. This option would help to ensure that enforcement agencies can use the most effective methods as technology and investigatory techniques develop, while still placing the protection of pre-authorisation and statutory criteria around their use.

Q8 Should the Act regulate a wider range of electronic surveillance (for example, surveillance using computer programs that track online activity, thermal imaging devices or chemical residue detectors)? If so, which types should be regulated and how?

In-person surveillance

3.77 In-person surveillance is not addressed at all by the Act, and has not historically been regulated.

3.78 By in-person surveillance we refer to activities carried out by enforcement officers themselves, rather than by electronic means, that involve observing or monitoring a person, place or thing. For example:

- an enforcement officer may follow a person in the street or sit outside their house in a car to observe their movements;
- an undercover officer may infiltrate a suspected criminal group or become associated with suspects in other ways, allowing the officer to access private premises or be privy to information that they could not access if their true identity was known; or
- an enforcement agency may ask an informant to monitor a person or obtain information on their behalf.

3.79 In New Zealand, the type of in-person surveillance that has attracted the most attention is the use of undercover police officers. In 2015 alone the Supreme Court heard three appeals concerning the admissibility of evidence obtained through police undercover operations in criminal investigations.[71]

---

[71] *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.

3.80 The use of evidence obtained through undercover operations can raise difficult issues, in part because the usual safeguards around warranted activity cannot be applied in the same way. For example, an undercover officer cannot advise a suspect of their rights before eliciting a confession without exposing the undercover operation. There have been instances of confessions being ruled inadmissible because they were obtained through active eliciting or interrogation by an undercover officer, in breach of the right to refrain from making a statement.[72]

3.81 Undercover operations also have the potential to involve breaches of the law by enforcement officers. This is problematic, particularly given that there is no general statutory authorisation for undercover activities (with the exception of drug offences, for which undercover officers have statutory immunity[73]).

3.82 In *R v Wilson*, for example, the Supreme Court considered a case where Police had forged and executed a bogus search warrant and launched a fake prosecution of an undercover officer to allay suspicion that he was a police officer. The Court found (and the Crown did not dispute) that this conduct was unacceptable in the absence of express statutory authorisation[74] and amounted to serious misconduct by the Police.[75]

3.83 The Supreme Court recently expressed support for the idea that some types of undercover activity may benefit from a more formal authorisation and supervision process. In *R v Wichman* the Court considered the use of the "Mr Big" technique, which involves a suspect being recruited by a bogus criminal organisation and persuaded to tell the "boss" about his past offending (on the basis that the organisation can resolve any problems associated with a possible prosecution). William Young J, giving the judgment for the majority, stated:[76]

> It is of note that court sanction in the form of a warrant is required for police investigations which are far less intrusive than a Mr Big operation. Against that background there may be some sense in devising a system (perhaps involving the courts) under which criteria for the deployment of such techniques are developed and perhaps for some form of supervision (perhaps in the form of a warrant process) to ensure that such considerations are properly weighed, where a proposed operation will be intrusive and may have damaging effects as far as the suspect is concerned.

---

72 See *R v Kumar*, above n 71.

73 Misuse of Drugs Act 1975, s 34A.

74 *R v Wilson*, above n 71, at [38].

75 At [91].

76 *R v Wichman*, above n 71, at [127].

Approaches in comparable jurisdictions

The United Kingdom's covert surveillance regime

3.84 In the United Kingdom, the Regulation of Investigatory Powers Act 2000 (UK) regulates covert surveillance (in addition to interception of communications and access to communications data). This potentially encompasses all of the types of in-person surveillance referred to in paragraph 3.78 above. "Surveillance" is defined as including:[77]

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device.

3.85 Surveillance is then separated into three types: "directed surveillance", "intrusive surveillance", and the use of "covert human intelligence sources".

3.86 Directed surveillance and intrusive surveillance cover in-person surveillance as well as the use of surveillance devices. If the surveillance involves an enforcement officer or a device being present on residential premises or in a private vehicle it is "intrusive"[78] and must be approved by a surveillance commissioner.[79] Surveillance that is not intrusive is classed as "directed" if it is for the purpose of a specific investigation and is likely to result in the obtaining of private information about any person.[80] This is likely to cover, for example, enforcement officers following a person's movements in public areas. Directed surveillance is approved at a senior level within the enforcement agency.[81]

---

77 Regulation of Investigatory Powers Act 2000 (UK), s 48(2).

78 Section 26(3). The surveillance must also relate to things taking place on the residential premises or in the private vehicle.

79 Intrusive surveillance is authorised by the Chief Constable or Commissioner of Police of the relevant police force (s 32(1)) but must be approved by a surveillance commissioner (a former judge) before the authorisation takes effect (s 36).

80 Section 26(2).

81 Directed surveillance can be authorised by a "designated person", which means a person of a particular position or rank (designated by the Secretary of State) within the relevant public authority: ss 25(2) and 28. Authorisation is not required if the surveillance is an immediate response to events or circumstances and it would not be reasonably practicable to obtain authorisation: s 26(2)(c).

3.87 The United Kingdom's approach to "covert human intelligence sources" (CHIS) is of particular relevance. The use of a CHIS involves inducing, asking or assisting a person to:[82]

- establish or maintain a relationship with another person for the covert purpose of doing or facilitating one of the things referred to in the following bullet points;
- covertly use such a relationship to obtain information or to provide another person with access to information; or
- covertly disclose information obtained through the use or existence of such a relationship.

3.88 This can include the use of undercover police officers where they meet the criteria.[83]

3.89 The use of a CHIS can be authorised within the enforcement agency[84] unless it continues for more than 12 months, in which case the approval of a surveillance commissioner is required.[85]

3.90 Intrusive surveillance, directed surveillance or the use of a CHIS can be authorised where the authorising officer believes that the authorisation is necessary for the purpose of preventing or detecting serious crime, and that the proposed surveillance is proportionate to what is sought to be achieved.[86] Directed surveillance and the use of a CHIS can also be authorised for slightly broader purposes, such as preventing disorder or in the interests of public safety.

3.91 Before authorising the use of a CHIS, the authorising officer must also be satisfied there are certain specified arrangements in place for liaising with the source, overseeing the operation and keeping records.[87]

3.92 The Secretary of State is required to issue codes of practice on the exercise of powers and duties relating to covert surveillance.[88]

---

82 Section 26(7)–(8).

83 See Home Office *Covert Human Intelligence Sources: Code of Practice* (December 2014) at [6.6].

84 Regulation of Investigatory Powers Act 2000 (UK), ss 29–30.

85 Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 (UK), cls 3 and 5.

86 Regulation of Investigatory Powers Act 2000 (UK), ss 28, 29 and 32.

87 Section 29(2) and (5).

88 Section 71; Home Office *Covert Human Intelligence Sources*, above n 83.

Australia's controlled operations regime

3.93 Undercover operations are also regulated in Australia. The Crimes Act 1914 (Cth) creates a regime for authorisation of federal "controlled operations". These are operations investigating serious crime that may involve a law enforcement officer in conduct that would otherwise amount to an offence.[89]

3.94 Controlled operations are authorised internally within Police. Usually, they can be authorised by the Commissioner of Police, a Deputy Commissioner or any senior executive member authorised by the Commissioner.[90] However, they must be authorised by the Commissioner or a Deputy Commissioner if they will:[91]

- involve the infiltration of an organised criminal group by one or more undercover law enforcement officers for a period of more than seven days;
- continue for more than three months; or
- be directed against suspected criminal activity that includes a threat to human life.

3.95 The legislation sets out a list of criteria that must be met before a controlled operation can be authorised. Among these are that the operation must relate to specified offences punishable by three years' imprisonment or more, any unlawful conduct must be minimised, and the operation must not be carried out in a way that will induce people to commit offences or endanger the life or safety of any person.[92]

3.96 The controlled operations regime also confers immunity from criminal liability and indemnity against civil liability to officers acting in accordance with an authorisation.[93]

3.97 Another part of the Australian Crimes Act establishes a related internal authorisation regime facilitating the creation of assumed identities to support covert operations. This can be authorised where it is necessary for the purpose of investigating or gathering intelligence about criminal activity.[94] The authorisation can require government agencies and authorise non-governmental organisations to produce documentation

---

89 Crimes Act 1914 (Cth), s 15GD(1).

90 Sections 15GI and 15GF(1)(b) and (2).

91 Sections 15GD(2) and 15GF(1)(a).

92 Section 15GE.

93 Sections 15HA and 15HB.

94 Section 15KB.

supporting the assumed identity (for example, driver licenses and other identification documents).

Should in-person surveillance be regulated in New Zealand?

3.98 The nature of in-person surveillance—particularly in the case of undercover operations—can be equally intrusive or more intrusive than types of surveillance that require a warrant. For example, an undercover officer may form relationships with suspects and/or innocent third parties, be invited into people's homes and be included in private conversations on the basis of a misapprehension as to their true identity. Many people would likely consider this to be more intrusive than having their phone tapped or car tracked.

3.99 In-person surveillance may also result in obtaining similar types of information as the use of a surveillance device. An undercover officer may hear conversations that would otherwise need to be intercepted, or an enforcement officer may be able to track a person by following them in a car rather than using a tracking device. Equally, an undercover officer may enter private premises (on invitation), for which Police would otherwise require a search warrant.

3.100 Arguably, it is anomalous for the Act to be silent about in-person surveillance yet require warrants to use surveillance devices and carry out searches. Introducing an authorisation framework for in-person surveillance and undercover operations would help to ensure that proper consideration is given to the propriety and proportionality of a proposed approach before it is commenced. A statutory regime could also include standard conditions around the use of certain techniques. For example, it could specify internal procedures for the monitoring and oversight of covert operations. An authorisation would help to prevent breaches of suspects' due process rights and protect the privacy of individuals so far as possible.

3.101 As noted above, undercover operations have recently led to challenges to the admissibility of evidence. Prosecutions have failed as a result of these operations being carried out unfairly or unlawfully. Introducing an authorisation framework would help to ensure that State resources are only spent on setting up undercover operations in appropriate cases and that operations are carried out in such a manner that the evidence obtained is likely to be admissible.

3.102 Regulating in-person surveillance could also provide greater assurance to enforcement agencies and a clearer legal mandate. Currently, the lack of any legislative scheme can

leave enforcement agencies uncertain about what they can and cannot lawfully do. For instance, there are no general immunities for undercover officers,[95] since their activities are not authorised under the Act. But during the course of their work they may necessarily be implicated in criminal offending (such as where they are infiltrating a criminal enterprise).

3.103 There is also no regime in the Act for creating false identity information to support covert operations (such as false passports). There are some specific provisions in other legislation dealing with this, but only in relation to limited types of information.[96] We note that the New Zealand Intelligence and Security Bill 2016 would introduce a regime for the creation and use of assumed identity information by the New Zealand Security Intelligence Service and Government Communications Security Bureau.[97] A similar regime may be appropriate for Police and/or certain other enforcement agencies.

Q9 Should the Act regulate in-person surveillance (for example, watching a person's activities and/or using undercover officers)? If so, how?

Public surveillance

3.104 There is a range of ways in which enforcement agencies can monitor people using publicly available information or observing public areas. This type of activity has usually been treated as unobjectionable, given that it involves no more than doing what any member of the public could. However, the types of information that can be obtained in public places or from public sources is changing, as is its quantity and how it can be used.

3.105 The courts are now beginning to recognise that in some cases a person may have a reasonable expectation of privacy in things occurring in a public place. In *Hamed v R*, Blanchard J (with whom the majority agreed) accepted that public surveillance might invade a reasonable expectation of privacy if, for example, equipment was used that

---

95 Although, as noted above, there is a specific immunity for undercover officers in relation to drug offences (Misuse of Drugs Act 1975, s 34A).

96 See the Births, Deaths, Marriages, and Relationships Registration Act 1995, s 65 and the Land Transport Act 1998, s 24A.

97 New Zealand Intelligence and Security Bill 2016 (158-1), Part 3. See also 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), recommendations 78–81.

could capture more than the naked eye.[98] The Chief Justice would have gone further than that: she considered that people may well have expectations of privacy in public places if they reasonably believe themselves to be out of earshot or sight.[99]

3.106 The approach of Blanchard J was accepted by the Court of Appeal in *Lorigan v R*, which found that the use of a camera with night-filming capability to monitor a public street was a "search" under section 21 of NZBORA.[100] However, the Court considered the search to be lawful, on the basis that there was no statutory or common law rule prohibiting it.[101] The search was also found to be reasonable in the circumstances, because the expectation of privacy in activities occurring on a public street was relatively low.[102]

3.107 Notwithstanding that finding of lawfulness in *Lorigan*, our discussions with enforcement agencies suggested they are understandably reluctant to use techniques that might amount to a "search" for section 21 purposes, but for which a warrant cannot be obtained. The lack of clarity in the law about when such activities will be lawful means their use carries a higher risk that evidence obtained will be excluded.

3.108 Public surveillance raises distinct issues compared with other types of search and surveillance because it is often not targeted at obtaining evidential material relating to a specific offence. Instead, it may be undertaken for general screening purposes to detect any criminal offending that may be occurring. While the level of invasion of privacy may not be particularly severe when compared to a search of someone's home or mobile device, the number of people potentially affected is much larger.

3.109 This section discusses both public surveillance methods that are already used but are not subject to any regulation (such as CCTV), and some that are not in general use because it is unclear whether they are lawful (usually, because they could potentially amount to an unreasonable search under section 21 of NZBORA). We have addressed these two categories separately because bringing them within the ambit of the Act would have different implications. Regulating the former category would place greater scrutiny around activities that already occur, providing increased protection for

---

98 *Hamed v R*, above n 1, at [167].

99 At [12].

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

101 At [26]–[38].

102 At [39]–[45].

privacy rights. By contrast, bringing activities in the latter category within the warrant regime would expand the scope of police powers.

Public surveillance methods that could engage section 21 of NZBORA

3.110 There is an ever-increasing array of devices and techniques now available to law enforcement agencies that can be used in public places, but which disclose significantly more private information than can be gleaned by simply observing a person on the street. In addition to night-filming cameras, the thermal imaging devices and chemical residue detectors referred to above are examples of this. Although they may be employed in public spaces, they disclose information that could otherwise only be obtained by searching a person or their luggage or entering private property. As such, a court may find that they amount to a search and, depending on the circumstances, could breach section 21 of NZBORA.[103]

3.111 Another example is the use of detection dogs to screen people in areas accessible to the general public. Dogs can be trained to detect drugs, explosives, or even large quantities of cash. Currently detection dogs may be used by Police as an aid when executing a search warrant or exercising a warrantless search power.[104] However, the Act does not provide for general screening of public areas using detection dogs (for example, to detect drugs in schools or at train stations). While there does not yet appear to be any relevant New Zealand case law, the Supreme Court of Canada has held that the use of dogs in these types of circumstances invades a reasonable expectation of privacy.[105]

3.112 Currently, the public surveillance methods referred to above are not contemplated by the Act, so there is no ability for enforcement officers to obtain authorisation to use them. Although their use is generally not a criminal offence, it is possible a court would find that it breaches section 21 of NZBORA, depending on the circumstances. There is therefore a degree of uncertainty about the extent to which they may be lawfully used.

---

[103] As we have noted at paragraph [1.46] above.

[104] Search and Surveillance Act 2012, s 110(f).

[105] *R v AM* [2008] 1 SCR 569; *R v Kang-Brown* [2008] 1 SCR 456.

Public surveillance methods already in common use

3.113 There are some methods of public surveillance that are already in relatively common usage, both in New Zealand and overseas. For example:

- CCTV cameras are used to observe or record what is occurring in public areas in order to deter, detect or investigate crime;
- social media and other internet-based platforms accessible to the public are monitored by enforcement agencies for indications of offending; and
- helicopters are used to pursue suspected offenders fleeing crime scenes (in future, it is possible drones might fulfil a similar function).

3.114 The use of these kinds of methods has not generally been considered objectionable, as they simply allow enforcement officers to access information that any ordinary person could access. However, modern technology allows this type of public information to be gathered in large volumes, aggregated and used in increasingly sophisticated ways.

3.115 For example, if CCTV cameras are placed all over a city, the footage can potentially be used to track the movements of individuals in a similar way to a tracking device. As cameras become more advanced, the image may be of sufficient quality to be able to read text on people's devices or documents. Facial recognition software and automatic number plate readers are also now in use in some countries. These allow video data to be quickly processed and matched against government databases to identify potential offenders in a way that was previously impossible.

3.116 In October 2016, the Center on Privacy and Technology at Georgetown University's Law Faculty published a study on the use of facial recognition technology by Police in the United States.[106] The study found that the faces of over 117 million American adults were stored in law enforcement facial recognition databases. At least one out of four State or local police departments had the ability to run facial recognition searches. In addition, at least five major police departments had either claimed to run real-time facial recognition from street surveillance cameras, had bought the equipment for doing so or had expressed an interest in purchasing that equipment. The study expressed concerns over both the accuracy of facial recognition software and their lack

[106] Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law, 2016).

of regulation. It urged Congress and State legislatures to pass laws introducing thresholds for the use of the technology.

3.117 Another example of where sophisticated data aggregation and analysis can be used is social media monitoring. Computer algorithms are now available that can scan and filter social media and other internet-based material in a way that a person—or even a whole team of people—could not realistically achieve. These tools are already widely used by private organisations (for advertising and market research purposes, among others) and by some State enforcement agencies overseas. While they involve no more than making use of publicly available information, their potentially broad use by enforcement agencies to monitor the population at large could have a chilling effect on freedom of expression.

3.118 These types of developments mean that public surveillance techniques now have the potential to be more intrusive than they have been in the past.

3.119 In relation to CCTV, some countries—particularly in Europe—have decided that some form of regulation is appropriate. For example:

- In the United Kingdom, any processing of personal data (including the use of CCTV) must be registered with the Information Commissioner's Office, which maintains a public register.[107] The Secretary of State must publish a code of practice on the use of CCTV.[108] There is a Surveillance Cameras Commissioner who reviews and provides advice on the operation of the code, and encourages compliance with it.
- Spain has had laws in place since 1997 requiring prior authorisation by regional Commissioners of any use by Police of public CCTV.[109] The use of the camera must be necessary to maintain community safety.
- In Sweden, Police require a license from a county administrative board to install CCTV cameras.[110] The Board weighs the need to conduct CCTV surveillance in

---

107 Data Protection Act 1998 (UK), s 17. The public register can be searched at Information Commissioner's Office "Register of Data Controllers" <https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/>.

108 Protection of Freedoms Act 2012 (UK), Part 2.

109 LO 4/1997. See also Gemma Galdon Clavell, Lohitzune Zuloaga Lojo and Armando Romero "CCTV in Spain: An Empirical Account of the Deployment of Video-Surveillance in a Southern-European Country" (2012) 17 Information Polity 57 at 60–61.

order to prevent, detect or investigate crime against individual interests in not being watched.

3.120 In New Zealand, the use of CCTV cameras must comply with the principles in the Privacy Act 1993. For example, people must be alerted to the fact that cameras are in operation and there are certain requirements around how footage should be stored and used. These principles are of general application. The Privacy Commissioner has published guidance on how CCTV can be used by businesses, agencies and organisations in a compliant way.[111]

3.121 New Zealand Police has its own internal policy on the use of CCTV for crime prevention purposes.[112] It contains many principles that might be expected in a regulatory framework. For example, it specifies that cameras should only be installed in areas with a higher incidence of identified types of criminal offending than other similar areas, and should only operate during identified time periods when there is a higher likelihood of crime being committed. However, the policy is not binding and there is no mechanism for external approval or oversight of CCTV installation or use.

Should the Act regulate public surveillance?

3.122 When asking whether public surveillance should be regulated under the Act, it is important to distinguish between the two different types of public surveillance discussed above:

- The first category comprises activities that may (depending on the circumstances) breach section 21 of NZBORA – such as the use of search dogs, or drug or explosives detection devices, in public places. Currently these tools could be used to facilitate a search where an existing search power exists, but the Act does not provide for their broader use to screen members of the public. Recognising these types of activities as legitimate in the Act would increase law enforcement powers (albeit subject to statutory standards and authorisation requirements).

---

110 Swedish Camera Monitoring Act 2013:460. See also Swedish National Council for Crime Prevention *CCTV Surveillance of Stureplan and Medborgarplatsen: Interim Report 2* (2014) at 2.

111 Privacy Commissioner *Privacy and CCTV: A Guide to the Privacy Act for Businesses, Agencies and Organisations* (2009).

112 New Zealand Police *Crime Prevention Cameras (CCTV) in Public Places Policy* (May 2010).

- The second category comprises activities that are already carried out on the basis that they are not a "search", such as CCTV and social media monitoring. Regulating these types of activities would have the opposite effect: it would place restrictions on methods that are already in common use. This would help to ensure those methods are only used where appropriate, but may also risk unduly constraining law enforcement activities.

3.123 As we have noted, public surveillance is fundamentally different from the types of search and surveillance permitted under the Act in that it is usually not targeted at a specific individual or offence. As the Canadian Office of the Privacy Commissioner has said in relation to CCTV:[113]

> Video surveillance of public places subjects everyone to scrutiny, regardless of whether they have done anything to arouse suspicion. At the very least it circumscribes, if it does not eradicate outright, the expectation of privacy and anonymity that we have as we go about our daily business.
>
> The medium's very nature allows law enforcement to observe and monitor the movements of a large number of persons, the vast number of whom are law-abiding citizens, where there are no reasonable grounds to be capturing a record of their activities.

3.124 The Law Commission previously considered whether CCTV use should be regulated in its 2010 Report, *Invasion of Privacy: Penalties and Remedies.*[114] It recommended against introducing specific legislation dealing with CCTV or requiring authorisation or licensing for CCTV systems. Instead, it recommended that CCTV continue to be regulated by the Privacy Act. However, that Report was focused on remedies for breaches of privacy generally, rather than surveillance for law enforcement purposes. Regulation of CCTV was therefore considered in relation to all CCTV systems, rather than those used solely for crime prevention and detection purposes.

3.125 An argument could be made that the use of public surveillance for law enforcement purposes raises different considerations, in light of the significant resources and coercive powers available to the State. If surveillance becomes too frequently used in circumstances beyond the investigation of specific offences (where a reasonable belief threshold must be met), the general public may feel they are being treated as suspects. This could have a chilling effect on the exercise of rights such as freedom of expression.

---

[113] Office of the Privacy Commissioner for Canada *Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (March 2006).

[114] Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at [4.9]–[4.18] and recommendation 19.

3.126 Regulating public surveillance techniques could help to ensure that they are only used where there is a demonstrable law enforcement need (for example, because the particular area of proposed use is associated with disproportionate levels of offending) that outweighs the public interest in being free from undue State interference.

3.127 On the other hand, surveillance or screening in public areas can help to protect against threats to safety and general public order. Provided it is used in a confined manner, it has the potential to be a valuable law enforcement tool that benefits society generally. Attempting to place statutory restrictions on public surveillance could reduce the effectiveness and responsiveness of enforcement agencies by increasing the administrative burden on them.

Options for reform

3.128 If public surveillance were to be regulated under the Act, the form of that regulation would likely need to be different to the current surveillance warrants and powers. The criteria for obtaining a search or surveillance device warrant are unlikely to fit the purpose of public surveillance, which is often focused on crime prevention and detection in a broader sense rather than investigation of a specific offence.

3.129 It is also likely that a warrant would not be the appropriate kind of authorisation, particularly in relation to activities such as CCTV and social media monitoring that are already lawfully carried out. It may be preferable to have statutory criteria and/or a policy statement setting out the circumstances in which they can legitimately be used, and potentially (for CCTV, for example) an approval or registration requirement. This type of approach may better reflect the ongoing and generally lawful nature of the activity, and create less of a compliance burden for enforcement agencies.

Q10 Are there any types of public surveillance that should be regulated under the Act when they are used for law enforcement purposes (for example, social media monitoring or, in public places, the use of CCTV, detection dogs, facial recognition cameras or automatic number plate readers)? If so, which types should be regulated and how?

Q11 Are there other types of surveillance that should be captured by the surveillance device warrant regime in the Act?