MINISTRY OF JUSTICE
*Tāhū o te Ture*

LAW COMMISSION
TE AKA MATUA O TE TURE

# REVIEW OF THE SEARCH AND SURVEILLANCE ACT 2012

## ISSUES PAPER

November 2016, Wellington, New Zealand | NZLC IP40

**Law Commission**

Street address: Level 19, 171 Featherston Street, Wellington

Postal address: PO Box 2590, Wellington 6140, New Zealand

Document Exchange Number: SP 23534

Telephone: (04) 473-3453, Facsimile: (04) 471-0959

Internet: www.lawcom.govt.nz

**Ministry of Justice**

Street address (National Office): Justice Centre, 19 Aitken Street

Postal Address: DX SX10088, Wellington 6011, New Zealand

Telephone: (04) 918-8800, Facsimile: (04) 918-8820

Internet: https://consultations.justice.govt.nz

A catalogue record for this title is available from the National Library of New Zealand.

ISBN: 978-1-877569-77-7 (Online)

ISSN: 1177-7877 (Online)

This title may be cited as NZLC IP40.

This title is available on the internet at the Law Commission's website: www.lawcom.govt.nz

# Call for submissions

Submissions or comments (formal or informal) on this Issues Paper should be received by **16 December 2016.** Our final report and recommendations will be provided to the Minister of Justice by 28 June 2017.

You are welcome to make a submission in one of the following ways:

Completing an online survey at:
https://consultations.justice.govt.nz

Emailing your submission to:
ss1@lawcom.govt.nz

Posting your submission to:
Review of the Search and Surveillance Act 2012
Law Commission
PO Box 2590
Wellington 6140

**Your submission**

Submitters are invited to respond to any of the questions they have views on. It is not expected that each submitter will answer every question. Your submission can be set out in any format, but it is helpful to specify the number of the question that you are discussing.

We may refer to submissions in our final report. Please let us know if you do not want your name to be published. If you have any other privacy concerns, please contact us to discuss these before making a submission.

The Law Commission and Ministry of Justice may wish to discuss your submission with you. Please indicate in your submission if you are willing to be contacted for this purpose and specify your preferred method of contact.

**Official Information Act 1982**

The Law Commission and Ministry of Justice are subject to the Official Information Act 1982. Submissions on this Issues Paper will be made available on request unless there are specific grounds for withholding them. Any request for withholding of information on grounds of confidentiality or for any other reasons will be determined in accordance with the Official Information Act 1982.

# Table of Contents

# Summary of consultation questions

## CHAPTER 2 – THE SCOPE OF THE ACT

### Clarifying when a warrant should or must be obtained

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

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

### Defining the conduct that requires authorisation

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

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

(b) that the conduct targets a particular individual;

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

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

## CHAPTER 3 – SURVEILLANCE: AVAILABILITY OF SURVEILLANCE DEVICE WARRANTS

### The relationship between search and surveillance

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)?

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?

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?

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

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?

## CHAPTER 4 – SURVEILLANCE: INTERCEPTION AND TRACKING DEVICE WARRANTS

### Interception device warrants

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?

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

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)?

## CHAPTER 5 – SURVEILLANCE: EXECUTION OF WARRANTS

### Installing and removing surveillance devices

Q17 Should the Act provide for entry to premises other than the target premises to covertly install a surveillance device?

Q18 Should the Act provide for the removal of surveillance devices after the warrant has expired?

### Interception of incidental communications

Q19 Should applications for surveillance device warrants be required to identify:

(a) Any risk that a third party's communications will be intercepted?

(b) The process that will be followed to monitor or filter the intercepted material?

Q20 Should the Act impose a duty on a person intercepting communications to take all reasonable and practicable steps to minimise the likelihood of intercepting or listening to irrelevant communications?

Q21 How else might the Act address monitoring and filtering of intercepted communications?

### Retention of raw surveillance data

Q22 Should the Act recognise more exceptions to the requirement to delete raw surveillance data (for example, by permitting the retention of evidential material or associated data)?

## CHAPTER 6 – SEARCHING DIGITAL DATA

### Irrelevant and privileged material

Q23 Is there potential under the Act for enforcement officers or assistants searching digital material to see more material than is necessary for the purpose of the search (irrelevant material)?

Q24 Does the Act adequately protect privileged material from being seen by enforcement agencies during digital searches?

Q25 Are any amendments to the Act necessary or desirable to limit the amount of privileged or irrelevant material seen during electronic searches? For example, the Act could be amended to include:

(a) a requirement to document the search procedures followed and provide it to the owner of the material searched if requested;

(b) a requirement that the issuing officer consider the imposition of specified conditions designed to reduce the risk of seeing privileged or irrelevant material; and/or

(c) a duty on the person undertaking a search of digital material to take all reasonable steps to avoid seeing privileged or irrelevant material.

### Remote access searches

Q26 Should the Act continue to treat data stored remotely differently from data stored at a physical location that can be entered and searched?

Q27 Is it clear when specific authority for a remote access search is required? If not, what problems have you experienced?

Q28 If the Act continues to treat remote access searches differently, should it permit deferral of the requirement to provide notice after a remote access search has been conducted?

Q29 Should the Act be amended to facilitate access to evidential material stored overseas?

### Assistance to access computers and devices

Q30 Should the penalty for failing to provide access assistance be amended (for example, to explicitly provide for a fine as an alternative to imprisonment)?

## CHAPTER 7 – WARRANTLESS POWERS

Q31 Do the preconditions for the exercise of warrantless powers achieve the intended purpose and are they realistic to apply in urgent circumstances?

Q32 Should the Act expressly limit the use of warrantless powers to situations where it is not practicable to obtain a warrant?

Q33 Should warrants always be required for searches of electronic devices? If so, should there be an exception for urgent circumstances and/or a power to seize the device while a warrant is obtained?

Q34 Should the Act allow Police to enter a property to search for a person subject to electronic monitoring without a warrant, if there are reasonable grounds to suspect the electronic monitoring device has been tampered with?

## CHAPTER 8 – PRIVILEGE

### Should the Act provide greater protection for privilege?

Q35 Is privileged material adequately protected during the exercise of search or surveillance powers by the existing procedures? If not, what are the impediments to protecting privileged material?

Q36 Is it clear when and how privilege claims can be made?

Q37 Should the Act be amended to provide greater protection for privileged material? For example, by:

(a) requiring the enforcement officer applying for a warrant or order to identify potential issues of privilege; and/or

(b) requiring production orders and examination orders to explain the availability of privilege and how to claim it?

### The privilege against self-incrimination

Q38 Is there any scope for the privilege against self-incrimination (as described in section 60 of the Evidence Act) to apply to production orders? If not, should this be clarified in the Act?

Q39 Does section 130(3) adequately explain when the privilege against self-incrimination can be claimed?

Q40 Should section 130(3) be amended so that a person can decline to provide access information that is, itself, incriminating, in reliance on the privilege against self-incrimination?

## CHAPTER 9 – PRODUCTION ORDERS

Q41 Should the Act specify when a production order must be obtained?

Q42 Should enforcement agencies be required to report annually on the number of production orders they have applied for and the outcome of those applications?

Q43 Should the Act require or enable notification to a person whose information is disclosed under a production order?

Q44 If you do not favour notification, should the Act prohibit third parties from disclosing the fact of a production order to the person whose information is sought?

### Preservation orders

Q45 Is there a problem with data being unavailable by the time enforcement agencies have obtained a search warrant or production order?

Q46 Should the Act be amended to include a preservation regime? If so, do you have views on the design of that scheme?

## CHAPTER 10 – EXAMINATION ORDERS

Q47 Should the examination order regime remain in the Act?

Q48 Should examination orders be available in respect of persons suspected of, arrested for, or charged with the offending?

## CHAPTER 11 – THE USE OF INTELLIGENCE AGENCIES' CAPABILITIES FOR LAW ENFORCEMENT PURPOSES

Q49 Is there any justification for allowing intelligence agencies' capabilities to be used for law enforcement purposes beyond the current scope of police powers?

# Chapter 1 – Introduction

1.1 Search and surveillance powers are an essential tool in the armoury of the agencies that investigate and prosecute crime. Without those powers, much offending would go unprosecuted, many criminals would not be held accountable and our communities would be less safe.

1.2 However, it is just as important that those search and surveillance powers are designed to ensure they protect our human rights, particularly those rights relating to privacy, personal integrity, property and the rule of law. There is little to be gained by empowering agencies of the State to investigate crime if, in doing so, we erode the basic rights we value as a society and create fear or suspicion of the government among the very people it exists to protect.

1.3 The main purpose of the Search and Surveillance Act 2012 (the Act) is to facilitate the investigation and prosecution of offences in a manner that is consistent with human rights values.[1] This purpose does not set law enforcement and human rights values in opposition to each other; it suggests they are complementary. As the Law Commission said in 2007:[2]

> In our view, while there is a balance to be struck, there is also a good degree of complementarity between the two sets of values, particularly in a strong democratic state such as New Zealand. Search powers that encroach too far on human rights values are unlikely to gain legislative or community support. Similarly, investigative powers that are too tightly controlled and that prevent law enforcement officers from doing their job effectively will bring human rights norms into disrepute.

1.4 Balancing those complementary values remains at the heart of this review. However, as was apparent during the intense and extended public debate during the long passage of the Act, there is no clear agreement on how that balance should be struck. Opinions about the extent to which State intrusion into our lives is justified differ from person to person, depending in part on the nature of our personal experiences and beliefs.

1.5 For that reason, we wish to hear the views of as many individuals and organisations as possible. We hope that, through this consultation process, people will tell us where they think the right balance between law enforcement and human rights values lies.

---

1 Search and Surveillance Act 2012, s 5.

2 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [2.7].

## THE CONTEXT FOR THIS REVIEW

1.6 Search and surveillance powers form an integral part of many law enforcement investigations. In the 2014/15 reporting year, New Zealand Police exercised warrantless search powers on 7,048 occasions and obtained 122 surveillance device warrants.[3] Over 4,000 people were charged with criminal offences in partial reliance on the evidence obtained through the exercise of those powers.[4]

1.7 These statistics show the important role search and surveillance powers play in detecting and prosecuting crime, as well as the impact that the exercise of those powers has on individuals. This illustrates why it is crucial that the law ensures those powers are exercised in an appropriate way without unduly compromising the effectiveness of law enforcement investigations.

1.8 The statistics referred to in paragraph 1.6 do not include the number of search warrants that were issued, which we expect would be significantly higher in number than surveillance device warrants. Unlike warrantless searches and surveillance device warrants,[5] the Act does not require annual reports to include statistics on the number of search warrants issued. In addition, the numbers we have referred to only cover Police. As we discuss below, other government agencies also exercise search and surveillance powers.[6]

1.9 In a number of cases since the Act came into force, the exercise of search and surveillance powers has given rise to challenges to the admissibility of the evidence obtained in subsequent criminal proceedings. These cases demonstrate how the Act has been operating in practice in the courts.[7]

---

3 New Zealand Police *Annual Report 2014/15* at 148–148.

4 As above.

5 Search and Surveillance Act 2012, ss 170–172. Reporting is also required on examination orders and declaratory orders.

6 These agencies are also required to report on the use of warrantless powers and surveillance device warrants (Search and Surveillance Act, ss 171–172), but due to the large number of agencies we have not included those statistics here. As an example, in 2014/15 the New Zealand Customs Service obtained 16 surveillance device warrants and exercised warrantless entry or search powers governed by the Search and Surveillance Act on 34 occasions: New Zealand Customs Service *Annual Report 2014/15* at 93.

7 See *Rihia v R* [2016] NZCA 200 and *Birkinshaw v R* [2016] NZCA 220 for two recent examples of cases where evidence obtained through unlawful searches was nonetheless admitted; and *Ferens v R* [2015] NZCA 564 where the evidence was excluded. As we note in paragraph [1.47] below, there have been over 70 cases challenging the exercise of search and surveillance powers since the Act came into force.

## What the Act does

### *Consolidating search and surveillance powers*

1.10 The Act sought to bring the rules governing State intrusion on individuals' privacy for law enforcement and regulatory compliance purposes under one piece of legislation, as far as that could be done. It provides authority for the use of tools such as search warrants, surveillance device warrants, production orders and examination orders, and confers some warrantless powers on Police. It also controls how search powers are exercised.

1.11 The Act is not only concerned with police investigations. Some provisions in the Act also apply to other agencies that have powers of entry, search, inspection, examination or seizure conferred by over 70 different statutes. The people who exercise those powers are, along with police officers, referred to in the Act as "enforcement officers". While the search powers available to non-Police enforcement officers are set out in separate pieces of legislation, some provisions of the Act apply to their exercise.

1.12 The powers conferred on non-Police enforcement officers are often for the purpose of ensuring compliance with specific regulatory regimes. Enforcement officers include, for example, animal welfare inspectors, fisheries inspectors, product safety officers, food officers, forestry officers, gambling inspectors, immigration officers, inspectors of weights and measures, marine mammals officers, meat board auditors, park rangers, and wildlife rangers.

### *Controlling how information is gathered*

1.13 The search and surveillance powers falling within the Act's ambit enable enforcement agencies to gather information to assist in the investigation or prosecution of offending. That information—referred to in the Act as "evidential material"[8]—can take many different forms. For example, it may be visual (such as video footage from a surveillance camera at the scene of a drug deal), oral (such as the recording of a phone call that may refer to the sale of illegal drugs), written (such as financial records that show illegal transactions), physical (such as drugs found inside a house) or digital (such as emails on a computer or remote server that reveal illegal activity).

---

[8] Evidential material, in relation to an offence or suspected offence, means evidence of the offence, or any other item, tangible or intangible, of relevance to the investigation of the offence: Search and Surveillance Act 2012, s 3 (definition of "evidential material").

1.14 The Act regulates how this information is collected. In the examples given above, a surveillance device warrant could authorise the recording of the video footage and the interception of the phone call; production orders could require a bank to produce the financial records; and search warrants could enable the searching of the house, computer or remote server.

### *Providing checks and balances on the exercise of powers*

1.15 In addition to consolidating search and surveillance powers, the Act seeks to ensure that State intrusion on privacy for law enforcement purposes is closely regulated, able to be audited and only occurs where it is justified. It provides thresholds for the exercise of search and surveillance powers; requires prior judicial approval of intrusive actions, except in carefully defined circumstances;[9] and includes other safeguards such as reporting requirements.

1.16 These safeguards help to ensure consistency with section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA), which guarantees the right "to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise". This right will often have a role to play in auditing whether the tools provided in the Act have been legitimately or acceptably used. In most cases this auditing occurs when a defendant in criminal proceedings challenges the admissibility of evidence obtained under a search power.[10]

## What the Act does not do

1.17 The Act does not govern the powers of intelligence agencies, such as the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS). The powers of those agencies are set out in separate legislation and

---

[9] By "judicial approval" we mean approval by an issuing officer. "Issuing officer" is defined in s 3 of the Search and Surveillance Act 2012 as a District Court or High Court judge; or a person such as a Justice of the Peace, Community Magistrate, Registrar, or Deputy Registrar, who is for the time being authorised to act as an issuing officer under s 108 of the Act.

[10] The admissibility of the evidence is then determined under section 30 of the Evidence Act 2006. We discuss the relationship between section 30 and the Search and Surveillance Act below at paragraphs [1.46]–[1.52] of this Issues Paper.

have also been the subject of a recent review.[11] A Bill responding to the recommendations of that review is currently before a Select Committee.[12]

## The genesis of the Act

1.18 In 2001 the Law Commission was asked to "review the scope and adequacy of current powers to search persons and places and associated powers to seize in order to determine an appropriate balance between law enforcement [values] and the protection of individual rights".[13]

1.19 In its subsequent 2007 Report (which was the impetus for the Act), *Search and Surveillance Powers*, the Law Commission bluntly concluded that the existing law of search and surveillance in New Zealand was a "mess".[14] It was outdated, spread across numerous statutes, and there was significant variation in the tests for the exercise of powers as between Police and other enforcement agencies. The law also had not kept pace with technology.

1.20 The Commission observed that sometimes law enforcement agencies were constrained in terms of their enforcement role. At other times, their activity was completely unregulated, meaning that protections consistent with the rights affirmed in NZBORA were absent. Neither situation was satisfactory. Both drove the need to provide for a proper statutory framework, taking into account two sets of what the Commission termed "complementary" values: human rights and law enforcement values.[15]

1.21 Human rights values include the protection of privacy, personal integrity, property rights and maintenance of the rule of law. Law enforcement values reflect the public interest in detecting and prosecuting crime. The underlying principles of law enforcement include ensuring that powers are effective, simply expressed, certain in their exercise, and responsive (that is, able to meet different operational circumstances). Importantly, the protective rather than controlling role of law

---

11 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).

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

13 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at 19.

14 At 14.

15 At 20.

enforcement also requires consistency between the expression of those values and human rights values.[16]

1.22 That overarching balance was ultimately reflected in the detailed legislative purpose outlined in section 5 of the Act:[17]

> The purpose of this Act is to facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values by—
>
> (a) modernising the law of search, seizure, and surveillance to take into account advances in technologies and to regulate the use of those technologies; and
>
> (b) providing rules that recognise the importance of the rights and entitlements affirmed in other enactments, including the New Zealand Bill of Rights Act 1990, the Privacy Act 1993, and the Evidence Act 2006; and
>
> (c) ensuring investigative tools are effective and adequate for law enforcement needs.

1.23 The table below illustrates the lengthy process between the initiation of the Law Commission's original Search and Surveillance reference in 2001 and the enactment of the Search and Surveillance Act 2012. The public discussion that occurred over this 11-year period provides an important backdrop for our statutory review.[18] The table also shows that the process of drafting the current Act began as early as in 2007. There have been huge leaps forward in technology since then.

| PROCESS FROM INITIATION OF ORIGINAL LAW COMMISSION REFERENCE TO ENACTMENT OF THE SEARCH AND SURVEILLANCE ACT 2012 | |
|---|---|
| 2002 | The Law Commission published a Study Paper in March: *Electronic Technology and Police Investigations: Some Issues* (NZLC SP12). In April, the Commission also published a Preliminary Paper: *Entry, Search and Seizure* (NZLC PP50).[19] |
| 2007 | The Commission published its Report *Search and Surveillance Powers* (NZLC R97) and submitted the Report to the responsible Minister in June. |

16 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at 36–54.

17 What became s 5 of the Act was inserted into the Bill during the select committee process at the combined suggestion of the Law Commission and the Ministry of Justice, "to demonstrate explicitly that the Bill recognises the importance of human rights values". See the Search and Surveillance Bill 2010 (45-1) (interim select committee report) at 28.

18 There was heated public discussion around the proposed legislation throughout its passage, sparking a number of protests. Concern centred in particular on the proposed new warrantless powers, an integrated surveillance regime, the new production and examination order regimes, and the new residual warrant regime. Apart from residual warrants, which were reframed as declaratory orders, all those proposed regimes became part of the Act.

19 Law Commission *Annual Report 2001-2002* (June 2002) at 11–12.

| | |
|---|---|
| 2008 | The Search and Surveillance Powers Bill was introduced to Parliament as a Government Bill in September by the Labour Government. |
| 2009 | The Search and Surveillance Powers Bill was discharged in July. The Search and Surveillance Bill was introduced the same month by the National Government. The First Reading of the Bill occurred in August. |
| 2010 | The August interim report of the select committee released departmental and other supporting material and called for further written submissions. The final report of the select committee in November contained an extensive redraft of the Bill. |
| 2012 | The Bill was read for a second time in March. The Committee of the Whole House and the Bill's Third Reading took place the same month. The Bill received the Royal Assent in April. Most (but not all) of the Act's provisions came into force on 18 April.[20] |

## The structure of the Act

1.24 Part 2 of the Act empowers Police to apply for search warrants and examination orders, and confers an ability to conduct warrantless searches in some defined circumstances.[21]

1.25 Part 3 is directed to the powers of enforcement officers (whether Police or other officials) and confers the ability to apply for surveillance device warrants, declaratory orders and production orders.

1.26 Part 4 sets out general provisions in relation to the exercise of search, surveillance and inspection powers by any enforcement officer. So it applies both to powers conferred by Parts 2 and 3, and (at least in part) to the powers conferred on enforcement officers by other specified legislation.

1.27 The extent to which Part 4 applies to the exercise of a power by any non-Police enforcement officer is set out in the Schedule to the Act. The Schedule lists the powers in other legislation that all or part of Part 4 applies to, and the specific provisions of Part 4 that apply.

---

[20] Search and Surveillance Act 2012, s 2(1).

[21] Sections 6–44.

## THE SCOPE OF THIS REVIEW

### Issues that are within our scope

1.28 Our terms of reference (Appendix A) require us to consider the Act's operation since 1 October 2012. In particular, we were asked to consider significant case law and international developments relating to search and surveillance, as well as developments in technology and their broader implications. Our final report will provide recommendations on whether amendments to the Act are necessary or desirable.

1.29 This review was triggered by section 357 of the Act, which states:

> **357 Review of operation of Act**
>
> (1) The Minister of Justice must, not later than 30 June 2016, refer to the Law Commission and the Ministry of Justice for consideration the following matters:
>
> (a) the operation of the provisions of this Act since the date of the commencement of this section:
>
> (b) whether those provisions should be retained or repealed:
>
> (c) if they should be retained, whether any amendments to this Act are necessary or desirable.
>
> (2) The Law Commission and the Ministry must report jointly on those matters to the Minister of Justice within 1 year of the date on which the reference occurs.
>
> (3) The Minister of Justice must present a copy of the report provided under this section to the House of Representatives as soon as practicable after receiving it.

1.30 The departmental report provided to the Select Committee, which was produced during the passage of the Act, described the review process in section 357 as follows:[22]

> In addition to the safeguards of prior judicial approval, detailed reporting, and threshold requirements, the Bill provides for a comprehensive review of the Bill approximately five years after enactment. This recognises the significant changes in the area of search and surveillance that are effected by the Bill. … This provides an opportunity to review the Bill as a whole as well as the new powers contained within it to determine whether the Bill effectively protects the rights of individuals as well as meeting the operational needs of law enforcement and regulatory agencies.

1.31 In line with these comments, we consider that it is necessary to ensure, as far as practicable, that this review examines situations where the application of the current

---

[22] Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [48]–[49].

provisions is unclear or inconsistent, or where the balance between enforcement or regulatory objectives and individuals' rights needs some reassessment. However, this review is not designed to reopen the main policy decisions that underpin or are reflected in the legislation, unless there are readily apparent and significant problems that have arisen in the less than five years since the Act incrementally came into force.[23]

1.32 Although there is scope for improvement in some areas, particularly where changes in technology have had an impact, our overall impression so far is that the Act has provided greater clarity and consistency than the previous law. Where we have not identified any specific problems with provisions in the Act, we have not dealt with them in detail. This Paper instead focuses on those parts of the Act that appear to have given rise to operational difficulties or concerns about inadequate protection of rights. However, there may well be other issues with the Act we have not yet identified and we would welcome submissions on that.

1.33 Some parts of this Paper, particularly Chapters 2 and 3, do raise conceptual issues that have the potential to result in changes to the scope of the Act. We discuss these issues because enforcement agencies have highlighted real, practical problems that result from uncertainty in the current scheme of the Act. In particular, the lack of guidance as to when a search warrant must be obtained and the limited scope of the surveillance device warrant regime has led to uncertainty about the methods that enforcement agencies can lawfully use. This, in turn, has in some cases meant that enforcement agencies feel they are unable to use the most effective tools available to carry out their functions. Given these practical implications, we consider that addressing these issues falls squarely within our terms of reference and is in keeping with the purpose of this review.

### *Capabilities of intelligence agencies*

1.34 As we have noted, the Act does not in general govern the powers of intelligence agencies. However, there is a small degree of cross-over due to the fact that GCSB is able to provide assistance to Police within the scope of police powers.[24]

---

[23] Section 2 of the Search and Surveillance Act 2012 provides different commencement dates for particular parts of the legislation, with a final commencement date of 1 April 2014 for anything that was not brought into force before then.

[24] Government Communications Security Bureau Act 2013, s 8C.

1.35 In *Intelligence and Security in a Free Society*, the report of the First Independent Review of Intelligence and Security,[25] Sir Michael Cullen and Dame Patsy Reddy raised a particular question about whether the capabilities of GCSB and NZSIS should be able to be used for law enforcement purposes to a greater extent than under the current law.[26] As required by our terms of reference, this issue has been included in our review and is dealt with in Chapter 11. For reasons we discuss in that chapter, we consider no change to the current law is justified.

## Issues that are out of scope

### *Technical issues*

1.36 Given our terms of reference and the one-year deadline for our final report, we have not been able to address all of the issues that have come to our attention. We have taken the view that the main benefit of our joint review process is that it allows for broad public consultation. Therefore, we decided that our review should focus on the issues that would benefit the most from widespread public discussion. As our terms of reference reflect, these tend to relate to broader concerns around developments in technology, New Zealand case law and international practice in the nine years since the drafting of the Act began.

1.37 Other concerns, such as discrete drafting problems or matters that could be described as "technical", will be worked through separately by the Ministry of Justice and implemented at the same time as any reforms made as a consequence of this joint review. While we recognise that these types of issues can cause significant problems for enforcement agencies, in our view they would benefit less from broad public consultation.

---

25 Cullen and Reddy *Intelligence and Security in a Free Society*, above n 11.

26 The New Zealand Intelligence and Security Bill 2016 (158-1) introduced on 15 August 2016 implements the Government's response to Cullen and Reddy *Intelligence and Security in a Free Society*, above n 11. The Bill will replace the four Acts that currently apply to NZSIS, GCSB, and their oversight bodies with a single Act. That proposed legislation does not address the issue reserved for this review.

### *Bodily samples*

1.38 In addition to technical matters, this review will not deal with the issue of whether the general search warrant regime is an appropriate mechanism for seizing a bodily sample. This question was raised but not determined in *T v R*.[27]

1.39 This is because the Law Commission commenced a separate reference on the use of DNA in criminal investigations on 27 July 2016. This will involve a comprehensive review of the Criminal Investigations (Bodily Samples) Act 1995. It will also consider the relationship between that Act and the Search and Surveillance Act 2012. An issues paper will be published in relation to this reference in mid-2017.

## CONSULTATION

1.40 We conducted preliminary consultation in order to identify key problems with the current operation of the Act. This consultation was necessarily limited given the one-year time frame for the review. However, we attended over 30 meetings with enforcement officers, prosecutors, trial lawyers and other persons whose work engages the Act. We also held a combined meeting of officials and consulted with the judiciary, issuing officers, Internet specialists, privacy and human rights specialists, and the Commission's Māori Liaison Committee.

1.41 These preliminary discussions helped us to decide which issues to focus on in this Issues Paper. The submissions we receive in response to this Paper, as well as further meetings with interested parties as the review progresses, will help us to form our views on where amendments to the Act are needed and what form they should take. This will influence the recommendations that we make in our final report.

1.42 We have also established an Expert Advisory Group to assist us as we progress toward a final report. The members of this Group have been appointed for their individual expertise in the following fields – technology, digital security, privacy, human rights and criminal law.

---

[27] *T v R* [2016] NZCA 148.

## RECURRING THEMES

1.43 As we identified potential problems with the Act during our preliminary consultation, certain recurring themes emerged. These themes provide the backdrop to much of our discussion in this Issues Paper.

### The relationship between law enforcement and human rights values

1.44 The Commission in its 2007 Report stated that law enforcement values and human rights values are "complementary".[28] Despite that, the relationship between them is under pressure in terms of how the Act is implemented.

1.45 Much of that pressure comes from changes to technology and the way in which people use it, whether for lawful or unlawful purposes. The ubiquity of the smart phone, the rise of cloud computing, the automatic encryption of devices, the inevitable acquisition by enforcement officers of data that is not related to suspected offending – all these aspects place real stress on the balance between investigatory or regulatory needs and protection from State intrusion.

### The relationship between the Act and section 30 of the Evidence Act 2006

1.46 The Act contains a great deal of procedural detail about how search powers are carried out, but generally other legislative regimes determine what happens if there is a failure to adhere to those processes.[29] For example, successful challenges to the issue or execution of warrants or orders, or the exercise of search powers, may result in the evidence obtained from those flawed processes being ruled inadmissible in criminal proceedings.[30] Whether that will happen mostly depends on the exercise of a judicial discretion to exclude evidence under section 30 of the Evidence Act 2006, which is the regime for determining the admissibility of "improperly obtained" evidence.

---

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

29 One of the exceptions to this general statement about remedies is that where a claim to privilege is successfully upheld, the Act states that the communication or information to which the privilege applies is not admissible in any proceedings arising from, or related to, the execution of the search warrant or exercise of the other search or surveillance power or the carrying out of the examination or production order: Search and Surveillance Act 2012, s 148.

30 Sometimes a search warrant may be challenged by judicial review proceedings, particularly where no criminal proceedings are laid. However, this occurs in limited circumstances as there is usually no cross-examination in such proceedings and so the court has restricted fact-finding abilities, as noted in *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523 at [50]. In *Southern Storm Fishing (2007) Ltd v Chief Executive, Ministry of Fisheries* [2015] NZCA 38, [2015] NZAR 816 the Court of Appeal confirmed this should only be permitted where a fundamental defect has occurred in the process of issue or execution.

1.47 Challenges to the admissibility of evidence obtained through the exercise of search or surveillance powers are relatively frequent. A brief case law search suggests there have been over 70 such cases since the Search and Surveillance Act came into force, and the actual number is likely to be higher.[31]

1.48 The route to section 30 of the Evidence Act can be either direct or indirect. An example of the direct route is where a flaw in the application process for a search warrant means that the warrant was not lawfully issued. That might be because the grounds or conditions for issue (thresholds) have not been properly established in the application or because the warrant itself is so defective that anyone either executing or affected by it would likely be misled as to its purpose or scope. In either case the admissibility of the evidence gathered under the warrant can be challenged under section 30 of the Evidence Act.

1.49 An example of the indirect route is where a warrant is lawfully issued, but a judge nonetheless finds that it was executed unreasonably – thus breaching the right under section 21 of NZBORA to be "secure against unreasonable search or seizure". NZBORA contains no remedies, but a finding of unreasonableness will open up the exercise of the section 30 discretion to exclude the evidence obtained.

1.50 Exclusion of evidence is not a guaranteed result. Section 30 requires the court to consider whether the exclusion of improperly obtained evidence is proportionate to the impropriety of the way it was obtained. That balancing process is informed by giving appropriate weight to the impropriety but also by taking proper account of "the need for an effective and credible system of justice".[32] A number of non-exhaustive factors are listed in section 30 for the judge to consider.[33]

1.51 Throughout this Issues Paper we discuss whether section 30 of the Evidence Act is an appropriate mechanism for ensuring compliance with the Search and Surveillance Act. In particular, we discuss the fact that section 30 only provides a remedy for breaches of rights, rather than preventing breaches from occurring. In addition, it only applies where the legitimacy of a search is challenged in subsequent legal proceedings. This

---

31 A search on the *Westlaw NZ* online database for cases referring to section 30 of the Evidence Act and the Search and Surveillance Act returned 74 results. There are likely to be some District Court cases not included in these results.

32 Evidence Act 2006, s 30(2)(b).

33 Section 30(3).

raises the question of whether a greater level of rights protection is required at the point where a search is carried out.

1.52 However, this review is not concerned with the operation of section 30 itself. That will be considered by the Law Commission in a separate review of the Evidence Act that is due to commence shortly.[34]

## The application of the Act in regulatory contexts

1.53 The Law Commission's 2007 Report only considered search and seizure in the context of law enforcement. It did not address search or inspection powers in regulatory contexts – that is, search or inspection powers that "are enacted to secure regulatory compliance, and intended to be exercised in an environment where regulated activity is undertaken, and do not depend on the existence of a threshold before they are exercised".[35]

1.54 However, after the Law Commission's Report was published a decision was made to extend the operation of aspects of Part 4 of the Act to apply to powers exercised for regulatory compliance purposes as well.[36] Hence the Act is addressed to "enforcement officers", which includes not only police officers but also other officials (such as customs, internal affairs or fisheries officers) who have specified powers of entry, search, inspection, examination or seizure.[37]

1.55 In other words, the Act built on an existing legal structure for law enforcement, by overlaying general procedures for the exercise of those powers in both enforcement and regulatory (compliance) contexts.

1.56 On occasion this has created a less than comfortable operational fit. For example, parts of the Act are premised on the ability to obtain a search warrant, whereas some regulatory agencies have extensive warrantless powers of search or inspection and can

---

[34] This will be the second periodic review of the Evidence Act 2006, required by section 202 of that Act. The Law Commission expects to receive the reference by early 2017.

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

[36] Regulatory objectives involve conducting inspections, monitoring and enforcing compliance in particular industries or regulated fields, particularly where serious harm can occur from non-compliance (such as physical harm to people, harm to the environment, or damage to New Zealand's economy): *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) at 75.

[37] The Search and Surveillance Act 2012 only applies to persons other than constables if their powers are authorised by an enactment that appears in the Schedule to the Act or any other enactment expressly applying to provisions of Part 4 of the Act: see the definition of "enforcement officer" in s 3.

only obtain warrants in limited circumstances.[38] A number of the questions we identify in this Issues Paper have been raised by non-Police enforcement agencies. Their particular operational context and the manner in which their powers are conferred in other legislation give rise to different issues than those experienced by Police.

## THIS ISSUES PAPER

1.57 This Issues Paper explores the key areas where we consider the Act may benefit from amendment. It identifies some possible options for reform—if reform is considered desirable—and raises specific questions that we would like feedback on. It does not contain any recommendations; its purpose is to elicit comments that will assist us in reaching a final view.

1.58 We seek submissions on whether we have correctly identified problems with the operation of the Act and, if so, what changes should be made to address them. Submissions are open until 16 December 2016.

1.59 We use a number of specific terms in this Paper that are either used in legislation or relate to technological processes. We have footnoted statutory and technical terms the first time they are used. We have also collected the most frequently used terms in a glossary for ease of reference (Appendix C).

1.60 We also note that we are aware of some court cases relevant to the issues we discuss in this Paper that are subject to suppression orders. Where these suppression orders prevent us from referring to the content of the proceedings, we have either not referred to them at all or have simply noted (where it seems important to do so) that the issue is being considered by the courts.

1.61 We begin this Issues Paper with a discussion of some conceptual issues, as this influences our analysis throughout. Chapter 2 examines the scope of the Act, in terms of the type of conduct that it regulates. This chapter discusses the permissive nature of the Act, in that it enables enforcement officers to obtain warrants in certain situations but it does not usually explain when officers *must* obtain a warrant. It describes the uncertainty this causes and the implications that has both for the ability of enforcement officers to do their jobs effectively and for the protection of rights.

---

[38] For example, the Act only specifically provides for remote access searches in the context of search warrants (see paragraphs [6.106]–[6.108] of this Issues Paper).

1.62 Chapters 3, 4 and 5 look at particular issues that arise in the context of surveillance. Chapter 3 builds on the discussion in Chapter 2, by examining the availability of surveillance device warrants under the Act and whether a wider range of activities should be covered by the surveillance regime. We then explore specific issues with interception and tracking device warrants in Chapter 4. Chapter 5 has more of an operational focus. It discusses some of the practical difficulties that enforcement officers have encountered in the execution of surveillance device warrants.

1.63 The impact of recent developments in technology is a significant theme for this review. This is squarely at the heart of Chapter 6, which outlines an array of problems that stem from the way the Act deals with searches of digital material. The Act focuses heavily on how physical searches should be conducted. These rules are then applied by analogy to digital searches. This chapter looks at whether this approach should remain. It also considers how the Act should deal with access to remotely stored data.

1.64 In Chapter 7 we consider the powers to enter and search places, vehicles and things without a warrant and signal issues about their use and breadth. Among other issues, this chapter discusses the extent to which warrantless powers should be applicable to searches of electronic devices.

1.65 Our discussion of privilege in Chapter 8 ties into the important theme of whether the "complementary" nature of human rights and law enforcement values is appropriately reflected in the Act. We ask whether the Act should do more to protect privileged material from being seen during a search. We also discuss the privilege against self-incrimination and whether there is any scope for it to apply to production orders.

1.66 Then, in Chapters 9 and 10, we discuss two regimes that were considered new and controversial when the Act first came into force: production orders and examination orders. In relation to production orders, we ask whether the Act should be clearer about when a production order is required. We also seek views on whether a mechanism should be introduced for temporarily preserving data while a production order is obtained. To our knowledge, the examination order regime in the Act has never been used. We consider whether or not it should be retained.

1.67 The final chapter in our Issues Paper addresses the single issue that was referred to us as a result of the report of the First Independent Review of Intelligence and Security.[39]

---

[39] Cullen and Reddy *Intelligence and Security in a Free Society*, above n 11.

We examine the possible ways in which the capabilities of intelligence agencies could be used to a greater extent for law enforcement purposes. However, we indicate our initial view that no change to the current position is desirable.

# Chapter 2 – The scope of the Act

## INTRODUCTION

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

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

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

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

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

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

## THE CURRENT LAW

### What is a search?

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

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

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

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

---

1 Search and Surveillance Act 2012, s 6.

2 Section 110(a).

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

4 Section 6(a).

5 Section 103(j).

6 Section 103(h).

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

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

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

## Reasonable expectations of privacy

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

## What is surveillance?

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

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

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

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

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

---

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

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

21 Section 46.

22 Crimes Act 1961, s 216B.

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

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

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

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

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

---

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

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

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

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

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

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

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

## Declaratory orders

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

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

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

---

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

30 Section 66.

31 Section 65(1).

32 Section 65(2).

### *The legislative history of declaratory orders*

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

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

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

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

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

---

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

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

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

36 Recommendation 11.24.

37 At [11.121].

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

## HOW THE LAW HAS BEEN OPERATING IN PRACTICE

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

---

43 (22 March 2012) 678 NZPD 1245.

44 (7 March 2012) 678 NZPD 971.

45 (20 March 2012) 678 NZPD 1100.

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

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

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

## COMPARABLE JURISDICTIONS

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

### United Kingdom

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

2.46 Article 8 provides that:

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

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

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

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

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

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

---

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

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

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

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

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

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

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

55 Sections 26(2) and 28(2)–(3).

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

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

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

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

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

## Australia

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

64 Section 46.

65 Section 46A.

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

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

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

## Canada

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

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

---

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

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

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

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

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

72 Section 492.1.

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

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

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

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

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

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

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

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

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

---

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

76 Section 487.01(1).

77 As above.

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

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

80 At 160–161 (original emphasis).

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

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

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

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

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

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

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

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

## COMPARABLE LEGISLATION IN NEW ZEALAND

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

---

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

89 Government Communications Security Bureau Act 2003, s 15.

90 Section 15A.

91 Section 16.

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

93 Recommendation 41.

94 Recommendations 50–51.

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

96 Clauses 165–174.

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

## THE CASE FOR REFORM

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

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

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

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

---

97 See paragraphs [2.102]–[2.104].

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

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

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

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

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

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

## OPTIONS FOR REFORM

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

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

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

### Retain the status quo

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

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

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

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

### Clarify when a warrant should or must be obtained

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

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

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

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

### *Option 1: Introduce an optional residual warrant regime*

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

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

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

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

---

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

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

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

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

### *Option 2: Introduce a mandatory residual warrant regime*

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

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

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

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

---

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

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

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

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

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

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

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

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

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

## Define the conduct that requires authorisation

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

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

### *Current test: conduct that invades a reasonable expectation of privacy*

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

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

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

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

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

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

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

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

### *An alternative test: conduct that might engage privacy interests*

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

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

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

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

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

---

[103] See paragraph [2.106] above.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

105 At [167].

106 At [12].

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

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

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

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

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

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

(b) that the conduct targets a particular individual;

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

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

---

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

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

# 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?

# 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.

# Chapter 5 – Surveillance: Execution of warrants

## INTRODUCTION

5.1 This chapter considers practical issues arising from the execution of surveillance device warrants. This includes a discussion of the difficulties associated with installing and removing surveillance devices. We also explore concerns related to the extent of material obtained as a result of surveillance and its retention.

5.2 We note that we do not discuss the execution of search warrants (as opposed to surveillance device warrants) in this Issues Paper, except in the specific contexts of digital searches and privilege.[1] This is because our initial consultation and research has not raised any significant problems with the operation of the Act in this regard. However, if any readers are aware of problems with the operation of the search warrant provisions we would welcome submissions on that.

## INSTALLING AND REMOVING SURVEILLANCE DEVICES

### Crossing neighbouring land to install surveillance devices

5.3 Section 55(3) of the Search and Surveillance Act 2012 (the Act) requires a surveillance device warrant to specify (among other things):

> (d) the name, address, or other description of the person, place, vehicle, or other thing that is the object of the proposed surveillance: …
>
> (h) that, subject to section 45, an enforcement officer carrying out the activities authorised by the warrant may do any or all of the following, using any force that is reasonable in the circumstances to do so, in order to install, maintain, or remove the surveillance device, or to access and use electricity to power the surveillance device:
>
> (i) enter any premises, area, or vehicle specified in the warrant: …

5.4 An issue has been raised with us as to whether section 55(3)(h)(i) can permit access to a neighbouring property. It may be necessary for enforcement officers to cross neighbouring property in order to enter the place that is the subject of the surveillance without detection. For example, if a property that New Zealand Police wishes to surveil is known to have a security camera at the front entrance, officers may need to walk over a neighbour's lawn in order to access the property from the back.

---

[1] See Chapters 6 and 8.

5.5 The Law Commission's Report, *Search and Surveillance Powers*, recommended that the surveillance device warrant regime "should make it clear that, where necessary, the warrant authorises entry into third party premises and vehicles".[2] However, this is not explicit in the Act, nor is it clear from the Search and Surveillance Bill and associated materials whether it was Parliament's intent that entry onto third party premises should be permitted.

### *Options for reform*

5.6 As evidenced by the decision of the Court of Appeal in *Choudry v Attorney-General*,[3] the courts are reluctant to find that powers of entry are implied. Therefore, if it is considered that entry onto the land or premises of third parties may be justified in some circumstances, the Act should explicitly provide for it. The surveillance device warrant provisions could be amended to require warrants to specify any neighbouring properties that may be entered.

5.7 As a comparison, the Australian Surveillance Devices Act 2004 (Cth) specifies that a surveillance device warrant permits "the entry, by force if necessary, onto the premises, and onto other specified premises adjoining or providing access to the premises".

5.8 If enforcement officers were permitted to cross over neighbouring properties to install surveillance devices, that would clearly impact on the privacy of third parties who are not suspected of any wrongdoing. In most cases, however, the intrusion is likely to be on the lower end of the scale as the entry will be for a short period and confined to the curtilage of a property. In addition, there may be instances where Police are simply unable to carry out the authorised surveillance covertly without crossing a neighbouring property.

5.9 There are a number of protections that could be put in place to ensure that the level of intrusion on third parties' privacy is limited. For example, the Act could:

- Require surveillance device warrants (and applications for them) to specify the properties that will be entered, why that entry is required and the nature of the entry (for example, whether it will be confined to the curtilage of the property or

---

2 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.103].

3 *Choudry v Attorney-General* [1999] 2 NZLR 582 (CA).

involve entry of a building, and the anticipated duration of the entry). This would help to ensure that issuing officers assess in each case whether the proposed entry is justified and will be carried out in the least intrusive manner practicable.

- Require the persons executing the warrant to notify the owners or occupiers of the property concerned before entering, unless there is reason to believe this will prejudice the investigation (for example, because there is reason to believe the neighbour will alert the suspect). This would be consistent with the notice requirements for search warrants.[4]

Q17 Should the Act provide for entry to premises other than the target premises to covertly install a surveillance device?

## Removing surveillance devices after the warrant expires

5.10 The Act requires surveillance device warrants to state that entry onto premises is permitted in order to remove a surveillance device.[5] However, this only applies while the warrant is in force. The Act does not provide a process for entering premises to remove a device after the warrant has expired.

5.11 In most cases, enforcement officers cannot simply enter a property at any time they wish to remove a surveillance device. They will need to wait for an opportunity to enter without detection – for example, when they know that all of the occupants of a house are going to be out for a sufficient period of time. Such an opportunity may not arise in time to allow the surveillance device to be removed before the warrant expires.

5.12 While a further surveillance device warrant may be sought,[6] this will not always be appropriate. For example, the surveillance already carried out may have indicated that the subject is not in fact involved in any offending.

### *Options for reform*

5.13 Most comparable regimes in New Zealand and overseas provide for the removal of devices after a warrant expires, pursuant to a further warrant. The New Zealand Security Intelligence Service Act 1969,[7] the Canadian Criminal Code[8] and the

4 Search and Surveillance Act 2012, ss 131 and 134–135.

5 Section 55(3)(h).

6 Section 55(5).

7 New Zealand Security Intelligence Service Act 1969, s 4I.

8 Criminal Code RSC 1985 c C-46, s 186(5.2).

Australian Surveillance Devices Act[9] all provide for the issuing of removal or retrieval warrants authorising the removal of surveillance devices from a place or thing.

5.14 An alternative approach would be to include statutory authorisation to enter premises within a certain period of time after the expiry of a surveillance device warrant to remove the device. This would reduce the administrative burden associated with applying for a further warrant.

5.15 However, it would not allow an issuing officer to consider the circumstances surrounding the removal and, given those circumstances, whether or how the entry should occur. For example, depending on how much time has passed the occupants of the address may have changed. It may therefore be appropriate to seek consent from the new occupants to enter to remove the device, rather than entering the premises covertly. If a removal warrant was required, the issuing officer could take these types of considerations into account and impose appropriate conditions.

Q18 Should the Act provide for the removal of surveillance devices after the warrant has expired?

## INTERCEPTION OF INCIDENTAL COMMUNICATIONS

5.16 In the case of *Murray v R*, the Court of Appeal considered whether an interception warrant relating to specific named people could justify listening to all calls on a phone line.[10] The case involved appeals against conviction for methamphetamine manufacturing offences by two appellants, Mr Murray and Mr Yates. The relevant part of the judgment relates to the appeal by Mr Yates.

5.17 Mr Yates argued that evidence of intercepted phone calls relied on by the prosecution at his trial should not have been admitted. The phone calls were intercepted in reliance on a warrant that permitted interception of the calls of Mr Murray and a number of other named individuals who resided at the same address. Mr Yates was not identified in the warrant, nor were the two people who he spoke to in the relevant phone calls.

5.18 The issue on appeal was whether the evidence was obtained "in the course of carrying out activities authorised by a surveillance device warrant" so as to fall within

[9] Surveillance Devices Act 2004 (Cth), ss 22–26.

[10] *Murray v R* [2016] NZCA 221.

section 57 of the Act (which provides the surveillance equivalent of "plain view" seizure).[11] The Crown submitted that it was, because:

- It was operationally inevitable that the call would be intercepted. Where Police use an interception device on a phone line, all calls are recorded by the Crime Monitoring Centre (CMC), a national 24-hour monitoring service. CMC employees listen to all intercepted calls and summarise them.
- It was not possible to identify who the parties to a telephone conversation were without listening to each conversation.
- It was also not possible to tell without listening to the whole conversation whether the phone would be passed at some stage to a named suspect.

5.19 The Court saw some force in the argument that interception that is "operationally inevitable" is properly viewed as collected in the course of executing the warrant.[12] However, it considered it was only operationally inevitable that the beginning of each conversation would be listened to in order to identify who was on the line. The fact that the full conversations were listened to was a result of the police practice of using people to monitor interceptions who do not have the ability to identify the voices of the subjects of the warrants.[13]

5.20 The Court concluded:

> [152] Police should have introduced a step in their process to filter out those calls not involving a named suspect. Police could and should have organised themselves so that the initial analysis was undertaken by a staff member sufficiently briefed to undertake at least preliminary voice identification, so that conversations not involving one of the suspects could be identified as such, and set aside from further consideration.
>
> [153] What the law must strive for is some balance that recognises the operationally inevitable, but still gives due weight to the privacy interests of those who are not named suspects…

5.21 The Court rejected the argument that the situation was analogous to the inadvertent recording of conversations between non-suspects by a listening device installed in a room. It thought different considerations applied in such cases, "including the fact that

---

11 The "plain view" rule (s 123 of the Search and Surveillance Act 2012) is described below at paragraph [6.27]. In brief, it permits the seizure of items that are found incidentally during the course of a search, where the items could have been seized under a search warrant or search power.

12 *Murray v R* [2016] NZCA 221 at [146].

13 At [151].

the judicial officer issuing the warrant will have within their contemplation that the listening device will capture such conversations".[14]

5.22 Police told us that the decision in *Murray v R* is problematic from an operational perspective. Surveillance device warrants can be valid for up to 60 days, and may involve monitoring the communications of multiple people. This can require a considerable time commitment. It is unlikely to be efficient for investigating officers to perform that task.

5.23 In addition, arguably it is preferable for CMC employees to filter calls in the first instance, since they are independent from investigations. If the summary from CMC suggests a particular call has no relevance to the investigation, there will be no need for an investigating officer to listen to it.

5.24 The contrary argument, accepted by the Court of Appeal in *Murray v R*, is that the usual process adopted by Police involves a greater invasion of privacy than necessary because someone listens to the entirety of every intercepted phone call.

## Options for reform

### *Addressing the risk of incidental interception in warrant applications*

5.25 One of the Court of Appeal's concerns was that the issuing officer who issued the surveillance device warrant would not have been aware that the calls of non-suspects may be listened to.[15] One way of ameliorating this concern would be to specifically require each application for a warrant to intercept communications to identify:

- any anticipated risk that the communications of a person other than a named suspect will be intercepted (for example, because the interception relates to a landline in a house occupied by a number of people); and/or
- the process that will be followed to monitor and/or filter the intercepted communications.

5.26 This would allow an issuing officer to assess on a case-by-case basis whether interception and monitoring in the manner proposed is necessary and proportionate. It would also give the issuing officer the ability to impose any conditions necessary to limit the impact of the interception on third parties.

---

14 *Murray v R* [2016] NZCA 221 at [155].

15 At [155].

### *Imposing a duty to minimise the risk of incidental interception*

5.27 Alternatively, the Act could require a person acting under a surveillance device warrant or warrantless power[16] to take all reasonable and practicable steps to minimise the likelihood of intercepting or listening to communications other than those authorised by the warrant or power. We note that such a requirement applies to employees of New Zealand's intelligence agencies when they are carrying out interception.[17] It would also be broadly consistent with the Court of Appeal's decision in *Murray v R*. To facilitate this, it may be possible for CMC employees to be sufficiently briefed on specific investigations to be able to do preliminary voice identification.

5.28 The benefit of this approach is that it would help to ensure the privacy rights of third parties are protected (including where warrantless powers are exercised). However, it is also likely to increase the cost and/or reduce the effectiveness of police interception, since it would require voice identification of all calls at an early stage (even if the call may turn out not to be relevant or useful).

Q19 Should applications for surveillance device warrants be required to identify:

(a) Any risk that a third party's communications will be intercepted?

(b) The process that will be followed to monitor or filter the intercepted material?

Q20 Should the Act impose a duty on a person intercepting communications to take all reasonable and practicable steps to minimise the likelihood of intercepting or listening to irrelevant communications?

Q21 How else might the Act address monitoring and filtering of intercepted communications?

## RETENTION OF RAW SURVEILLANCE DATA

5.29 "Raw surveillance data" is the term used in the Act to refer to video and audio recordings, and full or partial transcripts of audio recordings.[18] The default position is that raw surveillance data can only be retained:[19]

---

16 See for example, s 48 of the Search and Surveillance Act 2012.

17 New Zealand Security Intelligence Service Act 1969, s 4F(1); Government Communications Security Bureau Act 2003, s 24.

18 Search and Surveillance Act 2012, s 3 (definition of "raw surveillance data").

19 Section 63(1).

(a) until any criminal proceedings have been concluded (and any appeal rights have been exhausted); or

(b) for a maximum of three years, if criminal proceedings have not been commenced but the data is required for an ongoing investigation.

5.30 A judge can make an order allowing retention for a further period, but only up to a maximum of two years.[20] In addition, a judge can make an order permitting ongoing retention of *excerpts* from raw surveillance data if satisfied they may be required for a future investigation.[21] Enforcement agencies can also retain, without any judicial order, information obtained from raw surveillance data that does not itself constitute raw surveillance data if it may be relevant to an ongoing or future investigation.[22]

5.31 Any raw surveillance data or information obtained from it that does not meet those retention criteria must be deleted unless it forms part of a court record.[23] The court record is only required to retain certain documents relating to the formal steps taken in a proceeding.[24] It does not include the evidence given at trial so is unlikely to include raw surveillance data in most instances.

5.32 Enforcement agencies have expressed concern that the requirement to delete raw surveillance data may create problems if a case is reopened at a later date. For example, David Bain and Mark Lundy were both retried on murder charges years after their original convictions. If something similar happened in a case where raw surveillance data had been relied on, the requirement to delete it may mean the evidence no longer exists and cannot be used in the retrial.

5.33 By contrast, forensic copies of data held in a computer system or data storage device need only be deleted if they do not contain any evidential material.[25] If a forensic copy does contain evidential material, it may be retained in its entirety. The ability to retain the *entire* copy (as opposed to only evidential material) is necessary for reasons of evidential integrity that may not apply to raw surveillance data.[26] However, it is still

---

20 Search and Surveillance Act 2012, s 63(2).

21 Section 63(3)–(4).

22 Section 63(6).

23 Section 64.

24 Criminal Procedure Rules 2012, r 7.2.

25 Search and Surveillance Act 2012, s 161(1).

26 See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.147].

noteworthy that there is no requirement to delete the copies once criminal proceedings have concluded. This suggests an intention that evidential material should be able to be retained indefinitely in case it is required for ongoing or reopened investigations.

5.34 The requirement to delete raw surveillance data was inserted into the Search and Surveillance Bill on the recommendation of the Select Committee. It appears the main concern of the Committee was the potential for retention of information that is not evidential material and relates to persons other than the suspects. The Committee explained:[27]

> Many surveillance operations involve the collection of large quantities of raw data, much of which will not be evidential material. … We are acutely aware of the fact that in such investigations, information will probably be collected about people who are innocent of any offending and we are conscious of the need to protect their privacy. We believe it is critical that the further retention and use of information for purposes beyond the immediate investigation be regulated in order to provide protection to such innocent people.

## Options for reform

5.35 It seems likely that the concern of the Select Committee to protect the privacy of individuals could be achieved while still allowing evidential material to be retained for the purpose of any subsequent reopening of an investigation.

5.36 The Act could be amended to allow enforcement agencies to retain evidential material and any associated information that, if removed, would compromise the integrity of the evidential material. Any other raw surveillance data would still need to be deleted. This approach would be consistent with the rationale underlying the provisions governing retention of forensic copies, as discussed above.

5.37 However, we note this may not entirely address the concern of Police. Where a case is reopened at a later date, it is possible that raw surveillance data not considered to be "evidential material" at the time of the original investigation will become relevant. Under the approach suggested above, this type of data is likely to have been deleted.

Q22 Should the Act recognise more exceptions to the requirement to delete raw surveillance data (for example, by permitting the retention of evidential material or associated data)?

---

[27] Search and Surveillance Bill 2010 (45-2) (select committee report) at 6.

# Chapter 6 – Searching digital data

## INTRODUCTION

6.1 Since the enactment of the Search and Surveillance Act 2012 (the Act) there has been an exponential growth in the storage of information in an electronic form. Much of daily life involves electronic devices of one sort or another – from reading books on devices, to driving cars fitted with GPS navigation systems, to monitoring our fitness with electronic wrist bands.[1] We communicate via text message, email and Skype. We keep up-to-date through social media and online news websites.

6.2 In addition, much data is generated in the background of our lives that we usually know little about. Cell phone towers track our movements, EFTPOS transactions track our spending habits and smart-meters track our electricity usage.

6.3 The storage of digital information is growing at exponential rates:

- Google now processes over 40,000 search queries every second on average, which translates to 3.5 billion searches per day and 1.2 trillion searches per year worldwide (up from nearly 800 billion searches in 2009);[2]
- a report prepared in 2014 for the United Nations Secretary-General on the data revolution noted that 90 per cent of data in the world had been created in the previous two years alone;[3]
- in New Zealand, the number of uncapped broadband data plans nationwide quadrupled from 2014 to 2015, while fibre-based Internet connections more than doubled;[4]
- in 2015, there were 117.7 wireless mobile broadband subscriptions per 100 New Zealanders;[5]

---

1 In this Paper we have used the term "electronic devices" in a broad sense to refer to all devices that operate with components such as microchips and transistors that control and direct electric currents. This includes but is not limited to computers, tablets and mobile phones.

2 Internet Live Stats "Google Search Statistics" <www.internetlivestats.com/google-search-statistics/>.

3 United Nations Secretary-General's Independent Expert Advisory Group on a Data Revolution for Sustainable Development *A World That Counts - Mobilising the Data Revolution for Sustainable Development* (United Nations, 2014).

4 From 115,000 to 628,000 and from 46,000 to 100,000+ respectively: Statistics New Zealand "Internet Service Provider Survey: 2015" (14 October 2015) <www.stats.govt.nz>.

- electricity smart meters have been installed in 1.2 million New Zealand homes, outnumbering traditional analogue systems.[6]

6.4 The rise in the use of mobile devices and remote data storage since 2012 has raised significant questions about the way the Act is operating. For example:

- Does the Act deal adequately with the risk of electronic searches capturing irrelevant or privileged material?
- Does the Act provide appropriate guidance in relation to remote access searching?
- Is the maximum penalty for failing to comply with a request to provide assistance to access a mobile device adequate?

6.5 This chapter discusses the similarities and differences between digital and physical searching, before considering each of these questions in turn. While we deal with issues that relate to privilege generally in Chapter 8, we have discussed privilege as it relates to the capturing of digital material in this chapter because some of the options for reform are shared with options to address the potential problem of seeing irrelevant material. It should also be noted that, in Chapter 7, we discuss whether New Zealand Police should be able to search electronic devices under warrantless powers.

## COMPARING PHYSICAL AND DIGITAL SEARCHES

6.6 The differences between digital and physical methods of data storage go further than merely the quantity of data stored on a digital device. There are also qualitative differences. For example, a smart phone can reveal the user's internet search history and where the user has physically been. If the owner of the phone is using some of the more common applications, their phone can reveal who their friends are, what they cooked for dinner, how much exercise they are doing, and how well they slept the previous night.

6.7 The nature and quantity of data about individuals now stored in electronic form presents opportunities for enforcement agencies but also challenges for the protection of human rights. Those challenges were recognised in the Law Commission's 2007

---

[5] Organisation for Economic Co-operation and Development "Wireless Mobile Broadband Subscriptions" <https://data.oecd.org>.

[6] Consumer New Zealand "What's a Smart Meter?" (14 August 2015) <www.consumer.org.nz/articles/smart-meters>.

Report, *Search and Surveillance Powers*.[7] The Commission considered whether computer searches have a potentially larger impact on privacy interests and require a more stringent search regime. It was thought that a person may be more concerned about a search of their computer than of their physical premises because of the large amount of personal information that may be present on the computer (rather than being dispersed around their premises in physical form). Also of concern was the potential for law enforcement investigators to see a large amount of material on a computer that is unrelated to the subject of the search.[8]

6.8 However, the Commission also considered that law enforcement investigators may not know in advance of executing a warrant whether the material sought is in electronic or physical form, meaning that a more stringent regime for computer searches may create an incentive for criminal organisations to use an electronic medium to conduct criminal activity.[9] Ultimately, the Commission concluded that:[10]

> … the fact that information is stored in intangible form should not confer any greater protection from search and seizure than information that exists in tangible form; on balance, a different regime for the search and seizure of intangible material is not justified.

6.9 This approach was largely adopted by the Act. The threshold for applying for and issuing a search warrant makes no distinction between whether the material is likely to be found in physical or electronic form.[11] Also, while the Act provides some specific provisions in relation to electronic searches,[12] many of the rules in the Act for the execution of warrants do not distinguish between electronic and physical search. That means that rules originally formulated in respect of physical searches must be applied by analogy to electronic searches.

---

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

8 At [7.14].

9 At [7.16].

10 At [7.19].

11 Search and Surveillance Act 2012, s 6. This provision reads: "An issuing officer may issue a search warrant, in relation to a place, vehicle, or other thing, on application by a constable if the issuing officer is satisfied that there are reasonable grounds—(a) to suspect that an offence specified in the application and punishable by imprisonment has been committed, or is being committed, or will be committed; and (b) to believe that the search will find evidential material in respect of the offence in or on the place, vehicle, or other thing specified in the application".

12 For example, more restrictive criteria for remote access searches and a duty on persons with knowledge of a computer to assist access to that system.

6.10 In many respects this approach is operating effectively. There seems to be no debate that the legal threshold for searching electronic material should be the same as for physical material. There are, however, some concerns around the practical application of the rules when a digital search is involved. This includes difficulties associated with:

- the increased likelihood of inadvertently capturing irrelevant or privileged material; and
- determining when and how the rules relating to remote access searches apply.

6.11 We discuss each of these concerns in this chapter. We also discuss a concern that has arisen as to the penalty for failing to provide assistance to access a computer.

## IRRELEVANT AND PRIVILEGED MATERIAL

### Digital searching methods

6.12 There is a range of ways of capturing electronic material. At one end of the spectrum, a portable electronic device can be connected to a terminal designed to screen the contents of the device for certain material. The New Zealand Customs Service uses this method to screen some devices for prohibited items or illegal activities at the border.[13] If the screening process does not detect any relevant material (for example, illegal pornography), the device is returned to the owner. No information from the device is copied or retained. This method involves a relatively low level of privacy invasion because most material on the device is not actually seen by a person and no data is retained.

6.13 In contrast, the content of a mobile phone carried by a person arrested or detained for an offence may be searched without a warrant if the arresting officer has reasonable grounds to believe that the phone contains evidential material related to the offence.[14] This may involve the officer manually searching the phone.[15] The search should be targeted to finding the particular information sought. A broad, untargeted search may

---

13 New Zealand Customs Service *Customs and Excise Act 1996 Review: Discussion Paper 2015* (New Zealand Customs Service, March 2015) at 132.

14 Search and Surveillance Act 2012, ss 88 and 125(1)(l).

15 However, Police tell us that manual searches are not generally recommended and that extraction devices, which capture all the data on a device, are provided in many centres.

be considered unreasonable by a court under section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA).[16]

6.14 Searches of computers and devices located at businesses and private homes, however, are generally conducted in a systematic manner involving two stages – first, capturing the data, and second, searching the captured data.

### *Capturing the data*

6.15 At the first stage, investigators will capture all the data stored on a targeted computer or device by making a forensic image of it. The images are either made on-site by downloading all the data onto a separate storage device; or off-site when the computers, devices or hard drives are seized and removed. The images include all the data on a computer or device, including deleted and hidden data. Investigators often use a write-blocking device to prevent the original material from being modified. Both the forensic image and the original data can be "hashed" using an algorithm. This means that the values assigned by the algorithm through the hashing process to the original data and to the forensic image can be compared to ensure that the image is accurate.

6.16 Enforcement agencies that undertake a large amount of digital searches often have digital forensic units (DFUs) with specialist computer forensic staff. These units exist independently from their organisation's investigating teams. Their functions are to capture the relevant computer data, search it for the specific information requested and send only the relevant material to the investigators. A key advantage of DFUs is that any irrelevant or privileged material inadvertently seen in the course of searching for the targeted material is not seen by the people actually conducting the investigation.

### *Searching the data*

6.17 At the second stage, the forensic image is searched for relevant material. Searches of digital material can be akin to searching for needles in very large haystacks and a variety of methods may be used to find the information sought under a warrant or when exercising a relevant search power. The process has been described to us as involving a combination of in-depth systematic search together with intuition and

---

[16] Section 21 of the New Zealand Bill of Rights Act 1990 reads: "[e]veryone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise".

experience. A forensic specialist will usually use specialist forensic software and search terms to find either the particular material targeted or to find material that is irrelevant and can be filtered out of the search.

6.18 Where the search is conducted by a DFU, any documents that appear to contain evidential material will be transferred to another storage device and sent to the investigating officers. Sometimes there will be a to-and-fro process between the investigators and DFU staff to clarify exactly what type of material is required for the investigation. Often a record of the search will be made, which includes the types of software and search terms used to isolate the evidential material.

## The statutory requirements

6.19 There are various ways in which the Act currently manages the risk of irrelevant or privileged material being seen by investigators undertaking digital searches.

### *Specification of details in warrants*

6.20 Reflecting the common law rule that warrants cannot be issued for "fishing expeditions",[17] there are a number of provisions in the Act that require the object of a search to be specifically described. This limits the amount of irrelevant material that will be seen. The application for a search warrant must provide certain particulars in "reasonable detail", including:[18]

> (d) the address or other description of the place, vehicle, or other thing proposed to be entered, or entered and searched, inspected, or examined:
>
> (e) a description of the item or items or other evidential material believed to be in or on the place, vehicle, or other thing that are sought by the applicant:

6.21 The particulars that must be described in the warrant itself include:[19]

> (f) the address or description of the place, vehicle, or other thing that may be entered, or entered and searched, inspected, or examined:
>
> (g) a description of what may be seized:
>
> (h) the period during which the warrant may be executed, being—
>
> (i) a period specified by the issuing officer not exceeding 14 days from the date of issue; or

---

17 *R v Taylor* (1996) 14 CRNZ 426 (CA) at 433.

18 Search and Surveillance Act 2012, s 98(1).

19 Section 103(4).

(ii) if the issuing officer is satisfied that a period of longer than 14 days is necessary for execution, a period specified by the issuing officer not exceeding 30 days from the date of issue:

(i) any conditions specified by the issuing officer under subsection (3)(b):

(j) if the warrant may be executed on more than 1 occasion, the number of times that the warrant may be executed:

(k) if the warrant is intended to authorise a remote access search (for example, a search of a thing such as an Internet data storage facility that is not situated at a physical location) the access information that identifies the thing to be searched remotely:

(l) an explanation of the availability of relevant privileges and an outline of how any of those privileges may be claimed (where applicable):

…

6.22 The issuing officer may impose any conditions that are considered reasonable.[20] Those conditions could, in theory, include restrictions on how a search of electronic material must be conducted to minimise the risk of investigators seeing irrelevant or privileged material.

6.23 We note that there is no equivalent requirement for specification in relation to warrantless powers (as they are exercised without pre-authorisation by an issuing officer). Digital searches under warrantless powers are limited by the particular threshold for the exercise of each power and by the terms of section 110, which describes other powers that a person executing a search warrant or a warrantless search has.

### *The procedure for dealing with privileged material*

6.24 The law has long held that certain types of information are subject to heightened privacy interests and has granted them special status as privileged material.[21] The Act provides a framework for dealing with claims of privilege in respect of information that may be obtained under search or surveillance device warrants or other search powers. The purpose of that framework is to minimise the risk of investigators inadvertently seeing privileged material. In Chapter 8 we describe in more detail the procedure in the Act for dealing with privilege.

---

[20] Search and Surveillance Act 2012, s 103(3)(b).

[21] Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [122].

### *The rules governing seizure*

6.25 Prior to the Act, there was doubt surrounding the amount of data that could be captured in the first step of a search of digital material.[22] However, it is now clear that:

- the whole computer or device may be seized if it is not reasonably practicable to determine whether particular items on the computer or device are able to be seized;[23]
- reasonable measures may be used to access a computer system or other data storage device if intangible material that is the subject of the search may be on the computer or device;[24] and
- intangible material that can be seized can also be copied.[25]

6.26 Those rules reflect the fact that it can be difficult to know in advance exactly where on a computer or device the targeted material will be stored.

6.27 The Act provides no guidance on how forensic investigators must search the captured data for relevant material while minimising the risk of seeing privileged or irrelevant material.[26] However, there are rules applicable to all searches around what material may be seized that must be applied by analogy to digital searches. Generally, only items that are the subject of the search may be seized.[27] However, there has always been an exception for items related to criminal offending that are in "plain view", but are not covered by the warrant. The plain view rule was included (and extended) in the Act:[28]

> An enforcement officer to whom this section applies may seize any item or items that he or she, or any person assisting him or her, finds in the course of carrying out the search or as a result of observations at the place or in or on the vehicle, if the enforcement officer has reasonable grounds to believe that he or she could have seized the item or items under—

---

22 *The Chief Executive of the Ministry of Fisheries v United Fisheries Ltd* [2010] NZCA 356.

23 Search and Surveillance Act 2012, s 112.

24 Section 110(h).

25 Section 110(i). That would include copying the entire hard drive that was seized under s 112 because it was not reasonably practicable to determine on-site what items on the computer may be seized.

26 The Act lists some powers that are relevant to conducting electronic searches, such as the powers to request any person to assist with a search, to use equipment to help carry out a search and to use reasonable measures to access a computer system or other data storage device (s 110(b), (e) and (h)), but they do not restrict or guide how the search may be conducted.

27 Section 110(d).

28 Section 123(2).

(a) any search warrant that could have been obtained by him or her under this Act or any other enactment; or

(b) any other search power exercisable by him or her under this Act or any other enactment.

6.28 The plain view rule does not affect the scope of the search itself; rather, it dictates what items found during a search can be seized. In effect, section 123 means that enforcement officers may seize items that come to light incidentally during the course of a search that are relevant to a different offence. However, no further searching can be undertaken to find further related items or to determine whether found items constitute evidential material (unless a different search power applies or a new search warrant is obtained).[29]

6.29 As we have discussed above, electronic devices can contain large amounts of information. Because of this, the "plain view" rule has the potential to operate more broadly in the electronic sphere than in respect of physical searches. There is a greater amount of material that an enforcement officer may "find" in the course of carrying out an electronic search and be able to seize under the plain view rule.

6.30 We do not see this as a problem with the plain view rule itself. It simply underscores the importance of ensuring that electronic searches are carried out in the most targeted way possible, to minimise the amount of irrelevant material that is seen.

### Does the Act permit enforcement agencies to see too much digital material?

6.31 There seems to be a concern, touched on in the Law Commission's 2007 Report,[30] that the sheer volume of information stored on a computer inevitably makes computer searches very intrusive. This concern equates the data captured to the data searched. However, a computer search is not inherently intrusive – it depends on how the search is conducted. If the evidential material sought is very specific and the search is well targeted for that material, it may be found with very little irrelevant material being seen, perhaps on par with a targeted search of physical premises.[31]

6.32 However, the nature of digital searches means that investigators can potentially see much more irrelevant material in the course of even a highly targeted search than would be usual for a physical search. Evidential material can be hidden, deleted or in

---

29 See Simon France (ed) *Adams on Criminal Law - Rights and Powers* (online looseleaf ed, Thomson Reuters) at [SS123.03].

30 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.14].

31 In fact, it could be argued that a well targeted search is less intrusive than a physical search of (for example) a home, which may include the bedroom and bathroom and is perhaps witnessed by the neighbours.

an unusual format, which means that investigators must sometimes search in areas of the hard drive that are not the most obvious places to find the material. For example, some businesses store documents as scanned photos or PDF files without converting them into text with optical character recognition.[32] In that situation, an investigator may need to search the photos on a computer to find the required evidence.

6.33 An understanding of the nature of digital forensic searches brings some perspective to this risk. Our research for this review and discussions with digital forensic specialists has led us to the following tentative conclusions:

- Digital searches generally capture much more data than the evidential material sought, but only a fraction of the captured data is actually seen.
- Searches of digital material are usually highly targeted to the evidential material sought. There is a legal requirement for the search to be targeted, but also the volume of data captured and pressures of time and resources generally make that a necessity.
- Just as in a physical search, investigators undertaking digital searches will see irrelevant material in the course of their search. In some cases, the potential to see irrelevant material is much greater in a digital search than in a physical search.

6.34 These are, however, preliminary conclusions and we would be interested to hear from those who conduct digital searches and those who have had their digital devices searched, as to whether our discussion in this chapter reflects their experience.

## Does the Act adequately protect privileged material during digital searches?

6.35 While the Act has gone a long way towards clarifying how issues of privilege must be dealt with when executing physical searches, it says nothing specific in relation to digital searches.

6.36 If a person claims privilege, the Act states that they must provide a particularised list of the things in respect of which the privilege is claimed.[33] A variety of practices have developed across the different enforcement agencies for dealing with this in respect of digital material. Often, the person executing the search will discuss the issue with the

---

[32] Optical character recognition (often known as OCR) is the mechanical or electronic conversion of images of typed, handwritten or printed text into machine-encoded text.

[33] Search and Surveillance Act 2012, ss 141(a) and 147(a).

person claiming the privilege and come up with a customised plan for identifying and then isolating the privileged documents. That plan may include:

- the owner of the material providing a list of search terms designed to identify privileged documents;
- a lawyer for either the person claiming privilege or for the enforcement agency trawling through the documents to identify legally privileged documents; or
- the appointment of an independent person to identify privileged material.

6.37 We note that the Inland Revenue Department (IRD) has established standard operating procedures for the use of its search powers, including dealing with privilege in digital searches.[34] Those procedures provide that:[35]

- electronically stored documents that are potentially subject to privilege will be copied or imaged, sealed and removed (or the device containing the document will be removed for imaging off-site);
- the copy or image will remain in the custody of IRD's DFU and not be released to investigators until after the privilege process is completed; and
- the owner of the documents can provide a list of keywords to the DFU staff, who will use them to identify documents to which the privileges apply.

6.38 We are told that the identified documents are then transferred to a separate storage device and offered to the owner to specify any documents for which they wish to claim privilege. Documents in respect of which privilege is claimed are permanently removed from the captured data.

6.39 These procedures and those described in paragraph 6.36 are particularly relevant where the entire contents of a hard drive of a computer or several computers are captured and searched, and more generally where there is no urgency. We would be interested to know how issues of privilege are dealt with in other circumstances, for example in relation to the search under a warrantless power of a single mobile device.

6.40 Finally, we note that some enforcement agencies have expressed frustration at the lack of legislative guidance on how to deal with privilege in digital searches, but also

---

[34] Inland Revenue Department *Operational Statement: The Commissioner of Inland Revenue's Search Powers* (OS 13/01, September 2013).

[35] As above at [136].

concede that any requirements need to be flexible enough to cater to different types of digital material and differing claims of privilege. Some agencies have also commented that privilege claims over digital material can cause significant delay in investigations.

## Options for reform

6.41 If it is concluded that the Act currently permits enforcement officers to see privileged material or more material than is necessary during digital searches, then there are numerous ways in which the Act could be amended to address that problem. We discuss three options for reform below.

### *Documenting search procedures*

6.42 One option for reducing the amount of irrelevant material that is seen during digital searches would be for the Act to require a person undertaking a search of a computer or other data storage device to produce a record of their search procedure. That record would then be available on request to the owner of the computer or device searched.

6.43 This option has three advantages. First, it would ensure that the person conducting the search is accountable for each step taken in the process. Knowing that someone may check up on the procedure followed should help ensure that the search is conducted within lawful limits. Second, it would provide a defendant in subsequent criminal proceedings with the means of checking whether or not evidence from the search used against him or her was lawfully obtained. Third, even if criminal proceedings did not eventuate, it would enable the person who owned the computer or device to know the extent to which his or her privacy had been interfered with and make a complaint to the Privacy Commissioner, where appropriate.[36]

6.44 This type of record is already part of the standard practice of DFUs within enforcement agencies and is provided as part of litigation disclosure to the defendant. We do not know the extent to which records are kept when computers or devices are searched by enforcement agencies without DFUs.

---

[36] Privacy Act 1993, s 67. Under this section, a person may make a complaint to the Commissioner alleging that any action is or appears to be an interference with the privacy of an individual. Under s 66 of that Act, an action is an interference with privacy if the action breaches an information privacy principle and, in the opinion of the Commissioner or Tribunal, the action caused loss, detriment, damage, or injury to the individual; adversely affected the rights, benefits, privileges, obligations, or interests of that individual; or resulted in significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.

### *Specifying example warrant conditions*

6.45 One option for both limiting the amount of irrelevant material that is seen and for preventing investigators from seeing privileged material would be for the Act to require the issuing officer to consider imposing conditions on the warrant that are specifically designed to address these risks.

6.46 As we have mentioned, issuing officers already have the power to impose any conditions on search warrants they consider reasonable. The Act provides two optional conditions as examples.[37] Further optional conditions could be added to that list in relation to digital searches (together with a requirement for the issuing officer to consider imposing such a condition), for example:

- requiring an electronic device that will be searched to be switched to "flight mode" as soon as it is seized;
- permitting only specified parts of the computer, data storage device, or data captured to be searched;
- permitting only specific search terms to be used to identify the information sought; or
- requiring the search to be supervised by an independent third party.

6.47 In relation to privilege, the issuing officer could be required to consider conditions covering how digital material should be handled to identify and separate out privileged material, along the lines of IRD's standard operating procedures.

6.48 The advantage of this option is that an independent person (the issuing officer) considers the risks of the digital search before the search is conducted – before privacy is invaded or the privileged material is seen. Requiring issuing officers to consider imposing specified conditions would help to balance the risks associated with search warrant applications being determined ex parte (meaning the issuing officer does not have the benefit of opposing submissions on what conditions are appropriate).

6.49 However, most issuing officers are not trained in the technical requirements for digital searches, which may limit the value of such an approach. There is a risk that these types of conditions could be imposed without a full understanding of their technical

---

[37] Search and Surveillance Act 2012, s 103(3)(b). The two optional conditions relate to restricting the time of execution and requiring assistance to be provided by the occupier or person in charge of a place searched.

impact, which could unreasonably reduce the flexibility available to investigating officers.

6.50 Also, each of the conditions relating to the risk of seeing irrelevant material in paragraph 6.46 may be of limited benefit:

- Switching a device to "flight mode" would prevent information accessible from the device via the Internet from being seen during the search. It would also ensure the information is preserved in the same form as when it was seized: if a device remains connected to the Internet, the data on it may automatically update or be over-written. However, we have been told that Police already recommend that officers switch mobile devices to flight mode to ensure the data cannot be remotely wiped or updated after it comes into police possession.
- Conditions limiting which parts of a computer or device can be searched or which search terms can be used may be very difficult to apply in practice, because it may not be known in advance how evidential material is stored on that computer or device. Also, data is sometimes deliberately stored in unusual formats to hide it from potential investigations. For example, the phone number of an associate could be in the contacts list on a phone, but could equally be in a word document stored on an email, in a photo or screenshot, or in an unrelated application. A suspect could use an abbreviation or nickname for an associate to make it harder for investigators to find material when using search terms.
- Supervision by an independent third party could be expensive and time-consuming. We have been told of instances where third parties have supervised digital searches, but only for the purpose of identifying privileged material. We suspect that, while the presence of a third party may provide reassurance to the owner of the material searched, it is not likely to have much impact on the amount of irrelevant material seen by investigators. In addition, it may pose a significant impediment to investigations.

6.51 While they are not completely independent, DFUs located within enforcement agencies offer a sort of compromise. As described above, they capture the data, search for relevant documents and send only those to investigators. While the forensic specialist may see significant amounts of irrelevant material, the actual investigators do not. However, there may be little point in a condition on a warrant requiring the search to be conducted by a DFU (where one exists within an enforcement agency), because we are advised that where that option exists it will be taken.

### *Statutory duty to take steps to avoid seeing privileged or irrelevant material*

6.52 A further option would be to impose a statutory duty on enforcement officers to take all reasonable steps to minimise access to privileged or irrelevant material. The Act currently places a similar duty in relation to privilege on any person who is undertaking surveillance under the Act. That person must: [38]

> … take all reasonable steps to prevent the interception of any communication or information to which a privilege recognised by this subpart would apply if the communication or information were sought to be disclosed in a proceeding.

6.53 We have no specific indication of the legislative intention behind the inclusion of this duty in relation to surveillance. However, we speculate that it was considered very difficult to enact specific procedures to protect privileged material in relation to surveillance, given that surveillance is an ongoing process that generally occurs without the subject's knowledge (and who is therefore unable to make a claim of privilege at the time it is occurring). By placing the onus on the person undertaking the surveillance to consider the issue in advance, some protection is provided and the flexibility that is required to undertake the surveillance is maintained.

6.54 In relation to searches of digital material, and merely for discussion purposes, a duty could be phrased as follows:

> Any person who undertakes a search of digital material must take all reasonable steps to avoid seeing:
>
> - material that is not evidential material to which the search power applies; and
> - any communication or information to which a privilege recognised by this subpart would apply if the communication or information were sought to be disclosed in a proceeding.

6.55 Such a duty would require the person undertaking the search to consider the two identified risks before undertaking the search and to implement procedures to avoid them. The advantages of this duty are that:

- it provides some assurance to the owners of the information searched that their privacy will not be unnecessarily invaded and that the risk of seeing privileged material is reduced;
- it recognises that the risks cannot be completely eliminated but that there is a public interest in officers taking steps to reduce the risk; and

---

[38] Search and Surveillance Act 2012, s 140(2)(a).

- the steps taken to mitigate the risks could be determined on a case-by-case basis, without prescriptive rules that might limit the flexibility required for a search.

6.56 We suspect that this duty would have little impact on large scale searches of digital material by DFUs of enforcement agencies. From what we are told, DFUs already take steps to address these risks in every case. We are less sure of the impact that it might have on one-off searches of digital devices by officers who are not forensic specialists. We envisage that "all reasonable steps" would require the officer to show that the search was planned and that it was targeted to the material sought under the warrant or search power.

Q23 Is there potential under the Act for enforcement officers or assistants searching digital material to see more material than is necessary for the purpose of the search (irrelevant material)?

Q24 Does the Act adequately protect privileged material from being seen by enforcement agencies during digital searches?

Q25 Are any amendments to the Act necessary or desirable to limit the amount of privileged or irrelevant material seen during electronic searches? For example, the Act could be amended to include:

(a) a requirement to document the search procedures followed and provide it to the owner of the material searched if requested;

(b) a requirement that the issuing officer consider the imposition of specified conditions designed to reduce the risk of seeing privileged or irrelevant material; and/or

(c) a duty on the person undertaking a search of digital material to take all reasonable steps to avoid seeing privileged or irrelevant material.

## REMOTE ACCESS SEARCHES

6.57 Prior to 2012, it was unclear whether a search warrant for computer information provided authority to access that information remotely.[39] The Act sought to address this by creating special rules for "remote access searches". A remote access search is defined in the Act as:[40]

> … a search of a thing such as an Internet data storage facility that does not have a physical address that a person can enter and search

[39] Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.74].

[40] Search and Surveillance Act 2012, s 3 (definition of "remote access search").

6.58 We discuss some issues with this definition below.[41] In practical terms, we have treated a remote access search as a search of material that is not stored on the computer or device being searched or on the same computer system as that computer or device.

6.59 The Law Commission's 2007 Report said that it was one of the most difficult issues it dealt with. It listed the Privacy Commissioner's concerns with the remote accessing of computer information as including:[42]

- the owner of the data is unable to be present during the search;
- the evidence obtained through a covert search of a computer is of questionable value unless the search is undertaken under carefully controlled conditions to ensure reliability and admissibility of evidence; and
- search warrants can be granted by people without the professional, legal and judicial experience required to craft appropriate conditions to protect the privacy of third parties.

6.60 The Commission cautiously concluded that the power to execute computer searches remotely "is not recommended as a general law enforcement tool".[43] However, it recommended there should be a power to access network computer data where it is accessible from a computer found at the place being searched; and to conduct remote access searches when there is no identifiable physical location where the data is stored.[44] These recommendations were generally implemented in the Act.

6.61 Since the enactment of the Act, the use of internet-based data storage facilities has grown exponentially. Both at home and in the office, web-based applications for business and conducting our private lives are in very common use. Some of the most common examples are Google Drive, Apple iCloud, Dropbox, Pinterest, and Xero accounting software. However, information is also stored on the Internet in ways we do not necessarily think of as "storage": for example, in email accounts, blogs, social media and many applications providing entertainment or services from our computers and devices.

---

41 See paragraphs [6.104]–[6.105].

42 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.106].

43 At 24.

44 At 24.

6.62 This increase means that it has also become much more common for evidential material required for law enforcement purposes to be stored on internet-based facilities. That raises a general question for this review as to whether the Act is clear enough about when searches of this Internet data require prior authorisation (or specific authorisation).

## The statutory provisions

6.63 The Act establishes separate rules for digital searches that are conducted remotely. However, the provisions tend to deal with remote searches in an indirect manner, making them somewhat difficult to understand. To start with, rather than defining "remote access search" directly, the Act defines the concept by reference to the condition for authorising it (it does not have a physical address that a person can enter and search).[45]

6.64 Just as the Act does not state when a search warrant is required, neither does it directly state when a warrant is required for a remote access search.[46] However, it does say that:

- an issuing officer must not issue a search warrant authorising the remote access search of a thing unless he or she is satisfied that the thing is not located at a physical address that a person can enter and search;[47] and
- if the warrant is intended to authorise a remote access search, it must contain the access information that identifies the thing to be searched remotely in reasonable detail.[48]

6.65 Strangely, those requirements are found in the section concerned with the form and content of a search warrant, rather than in the sections concerned with the contents of an application for a search warrant and with the conditions for issuing a warrant.[49] In effect, they mean that if a search to be conducted under a warrant is intended to

---

45 Search and Surveillance Act 2012, s 3 (definition of "remote access search": "a search of a thing such as an Internet data storage facility that does not have a physical address that a person can enter and search").

46 Although we note that a remote access search without a warrant may be an offence under s 252 of the Crimes Act 1961 (accessing a computer system without authorisation).

47 Section 103(6). Some people interpret this section as indicating a preference for physical searches.

48 Sections 103(4)(k) and s 3 (definition of "access information": "includes codes, passwords, and encryption keys, and any related information that enables access to a computer system or any other data storage device").

49 Sections 98 and 6.

include accessing material remotely, that remote access must be specifically authorised in the warrant. The Act says nothing about whether data can be searched remotely under a warrantless search power.

6.66 The Act states that any person executing a search warrant authorising a remote access search and any person called on to assist, may use reasonable measures to gain access to the thing and to copy any material found that is the subject of the search.[50] These powers replicate those provided in a standard search warrant. [51]

6.67 The only other provision in the Act that specifically deals with remote access searches relates to providing notice of the search. The person conducting a remote access search must provide notice of the search when it is completed by sending an electronic message to "the email address of the thing searched" providing specific details of the search and attaching a copy of the search warrant. If that electronic message is unable to be delivered, the person who conducted the search must take all reasonable steps to identify the user of the thing searched and to send the information to that person.[52]

6.68 Finally, it should also be noted that one of the standard powers of a person exercising a search power may enable some forms of remote access searching without requiring specific authorisation. Section 110(h) states that a person executing a search power has the power to use "any reasonable measures to access a *computer system* … located at the place" searched. The ambit of the term "computer system" (which is defined in section 3 of the Act) is fairly vague. However, to the extent that the computer system includes any data stored via an Internet facility, section 110(h) arguably enables remote access searching without requiring specific authorisation in a warrant. We discuss the meaning of "computer system" further below.

6.69 Our research and consultation to date raises three issues relating to remote access searches:

- whether there continues to be justification for separate rules for remote access searches, and if so:
    - whether the provisions in the Act should be amended to make the rules and their application clearer; and

---

50 Search and Surveillance Act 2012, ss 111 and 114.

51 Sections 110(h) and 113(2)(h).

52 Section 132.

- whether notice of a remote access search should be able to be deferred.

## The justification for separate rules is questionable

6.70 The principle underlying the special rules for remote access searches is a preference for physical searches, expressed as a requirement that an issuing officer may not authorise a remote access search unless there is no physical address that can be entered and searched. It appears that the purpose of this restriction is to allay any public concern over the apparent lack of protections around remote access searches:[53]

> … we expect that empowering enforcement agencies to conduct computer searches remotely would prompt widespread concern about authorised state hacking into the lives of private citizens (albeit under search powers) and that there would not be sufficient public confidence that privacy interests would be adequately protected.

6.71 Therefore, a key question for this review is whether public concern about access to remotely stored information remains high or whether it is thought that those concerns can be adequately dealt with procedurally – for example, by adequate particularisation of the database to be searched and notification requirements. Put another way, does a determination that the data sought is not located at a physical address that can be entered and searched mean that it should be subject to greater protection?

6.72 The Law Commission's original intention was for the legislation to indicate a preference for a physical search:[54]

> … where there are physical premises capable of being identified and searched, the presumption that a search power be exercised on those premises is to be preserved.

6.73 Therefore, if the subject of a search uses a dedicated computer to access an Internet data storage facility, a search of the internet-based data via that dedicated computer could be carried out when conducting a search (under a warrant or search power) of the physical premises where the computer is located. The search of the internet-based data would not need a separate, specific authority. However, where the search subject does not possess or use a dedicated computer to access the facility, and instead accesses the facility from any computer with Internet access:[55]

> … there is no specific physical location that can practicably be searched to locate a device that can then be subject to a computer search.

---

53 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.82].

54 At [7.83].

55 At [7.94].

6.74 The current problem is that since that policy was articulated in 2007, there has been a significant increase in the use of web-based applications for many purposes, both private and in business. That means that:

- the use of a dedicated computer to access internet-based applications has declined;
- a greater percentage of evidential material is found on internet-based data storage facilities;
- people are often unaware (and unconcerned about) where their data is stored; and
- the distinction between data stored locally and data stored remotely may not be clear to a law enforcement investigator.

6.75 Perhaps the key issue here is whether the location of the data should matter. Assuming data is located within New Zealand, should there be different rules for internet-based data that is not accessed from a dedicated computer (specific authorisation required) than for internet-based data that is accessed via a dedicated computer (specific authorisation is not required)? With the advent of cloud computing, does the location of the data stored become an artificial distinction?

### *Option for reform*

6.76 If it were thought that there should no longer be special rules for remote access searches, the Act could be amended to remove the requirement that an issuing officer may only issue a warrant for a remote access search if the thing to be searched is not located at a physical address that a person can enter and search. In other words, specific authorisation for a remote access search would not be required. Rather, applications for searches of remotely stored data would be governed by section 6 of the Act. That would mean that applications for search warrants relating to remotely stored data would not need to specify the access information for the thing to be searched.

6.77 The original intention behind the latter requirement was to prevent "fishing expeditions" by ensuring that remote access searches are confined to only what is justified for the investigation. However, arguably the requirements to adequately detail the scope of other types of searches would also provide sufficient protection for remote access searches. Applications for other searches must specify:[56]

---

[56] Search and Surveillance Act 2012, s 98(1)(d)–(e).

- the address or other description of the place, vehicle, or other thing proposed to be entered, or entered and searched, inspected or examined; and
- a description of the item or items or other evidential material believed to be in or on the place, vehicle or other thing that are sought by the applicant.

6.78 Under these requirements, instead of specifying the access information (for example, Google email; email address – joe.bloggs@gmail.com; password – 1234) the application for a search warrant would describe the thing to be searched and the evidential material believed to be in that thing (for example, "any emails to or from Joe Bloggs relating to the supply of illegal drugs on any ISP").

6.79 The current requirement to specify the access information can amount to a "catch-22" situation for enforcement officers: to get the access information, the officer needs to do a search, but in order to do the search, the officer needs the access information. Sometimes the officer is able to obtain access information from prior voluntary disclosure by a person, by using a production order, or from a prior unrelated search.

6.80 Relying on descriptions of the remote data sought, rather than on the access information for that data would remove a significant hurdle for criminal investigations. However, if the special rules for remote access searches are retained, there is scope to clarify the regime, as we discuss next.

Q26 Should the Act continue to treat data stored remotely differently from data stored at a physical location that can be entered and searched?

### The rules controlling remote access search are not clear

6.81 We have encountered some confusion as to when remotely stored data can be searched without specific authority and when a remote access search warrant needs to be issued by an issuing officer. This has resulted in a variety of practices amongst enforcement agencies:

- some agencies never do remote access searches because they are unsure about the meaning of "physical address";
- some agencies will access data stored remotely only from computers that are already open and logged on to the relevant database;
- sometimes any data that can be accessed from a computer located in premises that are being searched will be accessed (whether or not it is remotely located) if it falls within the terms of the search warrant; and

- some agencies restrict remote access searches to only those circumstances in which they can get a search warrant, making it unavailable to them in respect of warrantless powers (including search powers in other statutes).

6.82 This lack of clarity has been caused by several inter-related factors. We discuss each of these below and outline options that may help to address them.

### *Placement of the rules within the Act is confusing*

6.83 As noted above, the placement within the Act of the provisions controlling remote access searches is confusing. The key provisions are found in the section concerned with the form and content of a search warrant, rather than those concerned with the content of the application and with the conditions for issuing the warrant. This raises questions without clear answers about why these rules were separated out. What was Parliament's intention and does that different treatment have an impact on the interpretation of the provisions? We suggest that the placement of these rules creates unnecessary uncertainty as to their meaning.

### *The warrant regime is permissive not mandatory*

6.84 The Act provides rules for when an issuing officer may issue a search warrant authorising remote access search.[57] It says nothing directly about when a remote access search may be undertaken. However, enforcement agencies look to these provisions for indications of Parliament's intention as to when remote access search is permitted. It may be clearer and enhance the protection of privacy if Parliament's intention in this regard is stated more directly in the Act.

### Option for reform

6.85 To resolve this uncertainty, a new provision could be inserted into the Act that clearly specifies when a remote access search warrant is required. For example, it could be required if the thing to be searched is "any data not stored on the computer or device being searched nor on any computer connected to it".

6.86 Obviously, this raises the question of what is "connected" to the computer being searched. We discuss options for clarifying that concept in our discussion on

---

[57] Search and Surveillance Act 2012, s 103(6).

"computer system" below. There may also be other ways of describing the type of remote data for which a remote access search warrant is required.

6.87 We note that this issue is related to our discussion in Chapters 2 and 9 about whether the Act should be clearer about what types of search activity and requests for information from third parties should require a warrant or other authorisation. Any recommendation to provide greater clarity on those matters should be consistent with the approach taken in relation to remote access searches.

### *The meaning of "computer system" is unclear*

6.88 Section 110(h) of the Act states that a search power authorises the person exercising it:[58]

> … to use any reasonable measures to access a *computer system* or other data storage device located (in whole or in part) at the place, vehicle, or other thing if any intangible material that is the subject of the search may be in that computer system or other device.

6.89 This provision could be interpreted as authorising, without requiring further specific authority, access to data stored remotely, to the extent that data is part of the "computer system". This power applies to both searches under a search warrant or under a warrantless power of search.[59]

6.90 The key issue here is whether data stored via an internet-based storage facility is part of the "computer system" and, if so, whether that extends to Internet facilities that are public or controlled by an external person or organisation. One example of externally-controlled data stored remotely is Xero accounting software. Xero is a subscription-based accounting software tool for small to medium-sized businesses. In this system, all financial data is stored in the cloud and so can be accessed from any location and any computer. Does the storage of its financial data via an externally controlled Internet facility mean that it is not part of the "computer system" that the computer being searched is part of?

6.91 Unfortunately, the ambit of "computer system" is not clear. This is a problem because it means that it is also not clear what is authorised by the Act, what might be an

---

[58] Emphasis added.

[59] When a computer or device is searched under a warrantless power, data that is accessed remotely from that computer or device could be accessed without requiring further authority if it is part of the computer system to which that computer or device is connected. The warrantless search power does not authorise a search beyond that system.

unreasonable search under section 21 of NZBORA and what may be an offence under section 252 of the Crimes Act 1961 (accessing a computer system without authorisation).

6.92 The definition of "computer system" in the Act is borrowed directly from the Crimes Act:[60]

> **computer system—**
>
> (a) means—
>
> (i) a computer; or
>
> (ii) 2 or more interconnected computers; or
>
> (iii) any communication links between computers or to remote terminals or another device; or
>
> (iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and
>
> (b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.

6.93 The authors of *Adams on Criminal Law – Rights and Powers* consider that "computer system" extends to data on the Internet that is accessible from the computer being searched. The authors state:[61]

> A search of a computer network of a business, even though the server is at premises other than those being searched, is clearly contemplated by the definition. However, the definition would appear to be much broader and allow access to any web-based material that is accessible from a computer that is being lawfully searched. On this interpretation, a search of a Google account held by the owner of a computer in the premises being searched is permitted, whether or not the computer is logged on to Gmail at the time of the search and whether or not a password is required in order to access it.

6.94 Interestingly, the *Adams* commentary on the same definition in the Crimes Act (which is provided for the purpose of defining the ambit of certain computer crimes) dissects the definition and reaches slightly different conclusions on its ambit.[62] In relation to the phrase "interconnected computer", the authors suggest that there are two possible meanings, which depend on whether "interconnected" is measured by reference to the computer user or by reference to the operator or controller.

6.95 The first meaning is very broad. Under it, all the millions of computers that a user can access through the communication links of the Internet would be part of the computer

---

60 Crimes Act 1961, s 248; Search and Surveillance Act 2012, s 3.

61 *Adams on Criminal Law - Rights and Powers*, above n 29, at [SS3.09.01].

62 Simon France (ed) *Adams on Criminal Law - Offences and Defences* (online looseleaf ed, Thomson Reuters) at [CA248.03].

system, despite them being owned by diverse users, in different countries and operating to different technical specifications. The second meaning is much narrower. Under it, only the computers that are connected by the ability of a single person with appropriate authority within the system to determine how they operate would be part of the computer system. An example of this second meaning is a "local area network" of linked computers, which together provide computer services for a company, government agency or educational institution.

6.96 The authors of *Adams* suggest that the second, narrower meaning is more appropriate. This is because its focus on authorisation within the system ties into the lack of authorisation contemplated by the offences in the Crimes Act (such as the offence of unauthorised access to a computer system in section 252). Also, the broader meaning would make the concept of "communication links" used later in the definition redundant.

6.97 This raises a question about whether a broader or narrower interpretation of "communication links" is more appropriate in the context of the Act. If a wide meaning was adopted, that would capture the transfer of data to a cloud-based storage facility and would permit the searching of data remotely under section 110(h). If a narrower meaning was adopted, only data stored on other computers or devices able to be controlled by one authorised person (say within a local area network) could be accessed remotely under section 110(h). It would not cover data stored on the cloud.

6.98 This discussion demonstrates that at the very least, there is uncertainty about the ambit of "computer system", what sort of remote searching would be permitted under section 110(h), and what would amount to an unauthorised search in terms of section 252 of the Crimes Act.

### Options for reform

6.99 There is a variety of ways in which the Act could define the scope of remotely accessed data falling within the definition of "computer system". First, in theory, it could rule out all data not stored on the computer being searched. If that is the case, the person executing the search would have to first disconnect the computer from any Internet connection and then make an image of its hard drive. Any data accessible from that computer but not stored on it would not be accessible under the power in section 110(h). However, it would be open to the enforcement officer to apply for a

remote access search warrant. This option has the advantage of being very clear. However, it also introduces significant impediments to the investigation of offences.

6.100 Second, the definition of "computer system" could distinguish between data that is stored on an Internet storage facility that is internally controlled or externally controlled. For example, if an organisation stores some of its data via an internet-based facility that is controlled by it and solely for its own internal use, that data would be part of the "computer system". But data stored on an externally controlled internet-based facility (such as Xero) would not be part of that "computer system".

6.101 The appeal of this distinction between internally and externally controlled Internet data storage facilities is that the available data is clearly within the network of the computer being searched. However, it may also be thought to be a rather arbitrary distinction. The decisions as to whether an organisation uses an internally or externally controlled Internet system are likely to have little to do with how much control the organisation wishes to have over the information. It is likely to regard both types of data as being within its organisational system.

6.102 Third, the definition could distinguish remote data based on factors such as whether:

- the computer was currently logged on to that Internet facility at the time it was searched; or
- the Internet data storage facility is always only accessed from the computer being searched.

6.103 However, the first factor also provides only an arbitrary link to the computer being searched and it could be very difficult for the second factor to be determined by the person executing the search.

### *The meaning of "not located at a physical address" is unclear*

6.104 The Act uses the phrase "not located at a physical address that a person can enter and search" to determine when an issuing officer may provide specific authorisation for a remote access search.[63] However, the meaning of that phrase is somewhat vague. All electronic data (even that stored in "the cloud") is located on a server (or multiple servers) somewhere in the world. In theory, that place can be entered and searched, even if, in practice, that may not be practical. It is not clear whether the condition "that

---

[63] Search and Surveillance Act 2012, s 103(6).

a person can [not] enter and search" is satisfied only if it is literally impossible or whether practical concerns such as lack of time, lack of money, or the fact it is in another country or located in multiple places could make it not possible.

### Option for reform

6.105 If the preference for physical searches is to remain, the Act could at least be amended to be clear that the restrictions on the issuing of a warrant for remote access searches only apply where the thing to be searched does not have a physical address that can *practicably* be entered and searched. The introduction of this practicality element appears to reflect the original intention of the Act.

## *The ability to search remotely under warrantless powers is unclear*

6.106 As mentioned above, the provisions in the Act relating to remote access searches relate to search warrants only. There are no similar provisions relating to the exercise of warrantless powers. This leaves enforcement agencies unsure about whether or not they may access data remotely in those circumstances.

6.107 The main concern with the access of remotely stored data under warrantless powers is the risk of "fishing expeditions". While it is possible to adequately particularise the scope of a remote search in a warrant application (whether by providing the access information or other descriptions), there are no such checks on the exercise of warrantless powers. However, it may be possible to provide checks in other ways, for example, by reporting on the scope of the search after it has been conducted.

6.108 Of course, all warrantless search powers are exercised without a description of the scope of the search being approved in advance. This is justified because the thresholds for the exercise of warrantless powers require urgent circumstances: in other words, there is no time to obtain a warrant. Those thresholds themselves provide the check on the scope of the search. The question here is whether there is something unique about data accessed remotely that means that extra checks (over and above the existing thresholds for warrantless powers) are required, so that a warrant must always be obtained.

Q27 Is it clear when specific authority for remote access search is required? If not, what problems have you experienced?

## There is no ability to postpone notification

6.109 Currently, there is no ability to apply to a judge to postpone the notice requirements for remote access searches, as there is for searches of premises or vehicles when the owner or occupier is not present.[64] In those other cases, a judge may grant a postponement if satisfied that there are reasonable grounds for believing that providing notice as required would endanger the safety of any person or prejudice ongoing investigations.[65]

6.110 We have been told by enforcement officers that sometimes they obtain warrants for remote access searches at a point in time when it would be prejudicial to the investigation to require them to provide notice. This may be because the remote access search indicates the existence of data that may be evidence of the offence but was not covered by the first warrant. If notice is given at that point, the person to whom the search relates will be alerted to the investigation and may destroy any relevant evidence that has not yet been obtained.

6.111 We cannot see any reason to distinguish remote access searches from other types of searches on this basis. While remote searches are different in that (without being expressly notified) the operator of the database being searched often will not know about the search, the important point is that they are notified, not the timing of that notification. The justifications for deferring that notification therefore seem to apply equally to remote access searches as for other types of search.

### *Option for reform*

6.112 If it was thought that notification about a remote access search should be able to be deferred, that amendment could be incorporated into the existing power in section 134 to apply to a judge for a postponement of the notification obligation.

Q28 If the Act continues to treat remote access searches differently, should it permit deferral of the requirement to provide notice after a remote access search has been conducted?

## Information accessed remotely is often stored overseas

6.113 Finally, there is uncertainty about the ability of enforcement officers to access information stored on servers in other jurisdictions. Much evidential material from

---

64 Search and Surveillance Act 2012, s 134.

65 Section 134(3).

internet-based facilities will be of this nature – Google email accounts and Facebook postings are just two of the more common examples. Accessing data located in a different jurisdiction is likely to violate principles of customary international law, which prohibit law enforcement agencies from conducting investigations in other jurisdictions.[66]

6.114 In practice, third-party providers of Internet data services often comply with New Zealand law enforcement requests for data stored on servers in other jurisdictions, particularly if the provision of that data would constitute a minimal intrusion on privacy. However, in some cases there may be legal hurdles preventing the providers from complying. For example, in the United States the Stored Communications Act restricts the ability of telecommunications companies in that country to disclose the content of stored communications, including to foreign governments.[67]

6.115 If, for whatever reason, a provider refuses a request from a New Zealand enforcement agency, the agency may decide to continue the investigation as best it can without the information. Alternatively, it can embark on a request for mutual legal assistance under the Mutual Assistance in Criminal Matters Act 1992. Mutual assistance is a process that can facilitate the disclosure of information between countries for the purpose of investigating and prosecuting criminal offending. However, this process can be complex as different jurisdictions have different requirements that need to be satisfied before a request for mutual assistance will be entertained, and the process can sometimes take months to complete.[68]

### *The case for reform*

6.116 The general prohibition (under customary international law) on conducting investigations in the territory of another State presents challenges for law enforcement agencies that wish to access data stored on servers located in other jurisdictions. In our view, it is arguable that we need legal mechanisms both to provide law enforcement agencies with access to data stored in other jurisdictions where this is appropriate, and

---

66 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.109].

67 Stored Communications Act 18 USC § 2702.

68 Jennifer Daskal and Andrew Keane Woods "Congress Should Embrace the DOJ's Cross-Border Data Fix" Lawfare <www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0>.

to ensure that the privacy of data stored in this country is adequately protected from requests for access from law enforcement agencies in other jurisdictions.

6.117 This issue arose in a recent high profile case in the United States. In *Microsoft Corporation v United States of America*, federal law enforcement officers investigating drug offences sought and received a search warrant under the Stored Communications Act for email account information about a suspect held by Microsoft.[69] Microsoft provided some account data that was held on servers in the United States. However, it refused to supply content data that was stored on servers in Dublin, Ireland on the basis that the data was beyond the territorial control of the law of the United States.

6.118 The question for the court was whether the warrant applied extraterritorially. The United States Government argued that the warrant required Microsoft to disclose the relevant records that were under its custody or control, no matter where those documents were located. Microsoft argued that warrants have territorial limits and do not extend to things located in other jurisdictions.

6.119 The Second Circuit Court of Appeals held that there was nothing in the Stored Communications Act that indicated an intention for the warrant to operate extraterritorially; and that the conduct in question (supplying the information) would occur overseas despite the fact the information could be accessed from the United States. In holding that Microsoft could not be compelled to produce the email information stored in Dublin, it said:[70]

> Although the Act's focus on the customer's privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the [Act] where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government.

6.120 In reaching this conclusion, the Court emphasised that retrieving the data will necessarily require interaction with the Dublin data centre, which is located in a foreign sovereign State. While the Court recognised that its decision would seriously impede law enforcement investigations, it said the practical considerations did not overcome the interpretation that the warrant could only reach data stored within the United States.

---

69 *Microsoft Corporation v United States of America* 829 F 3d 197 (2d Cir 2016).

70 At 220.

### *Options for reform*

6.121 At first glance it may seem that the logical solution to the problem of New Zealand enforcement officers not being able to readily access data stored overseas would be to amend the Act to give production orders extraterritorial effect. This could be done by specifying that the obligation in section 75(1) to disclose any relevant documents that are in the person's possession or control extends to documents located in other jurisdictions. In practice, however, this would likely be unenforceable. The service provider in the foreign country might not be obliged to disclose the information and would be subject to the law of the foreign country.

6.122 An alternative solution adopted by some countries (notably Russia and Brazil) would be to enact a law that requires any company providing a service to New Zealand citizens to store all the related data in New Zealand.[71] While the primary policy behind such a law is to protect citizens' data from unauthorised access by foreign governments, it would also ensure that data generated by citizens is available to New Zealand's enforcement agencies. However, data localisation policies have been criticised as being ineffective (data security is better protected by encryption than localisation) and as deterring growth and innovation due to the extra costs these policies impose on companies.[72]

6.123 The most viable option for addressing the issue of cross-border access to data may involve international cooperation. The leading international instrument in relation to this type of cross-border assistance is the Budapest Convention.[73] The Budapest Convention is a multilateral treaty adopted by the Council of Europe in 2001. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties. Chapter III of the Convention deals specifically with international cooperation and includes obligations relating to preservation (and limited disclosure) of stored

---

71 Vindu Goel and Andrew E Kramer "Web Freedom Is Seen as a Growing Global Issue" *The New York Times* (online ed, New York, 1 January 2015); and Loretta Chao and Paulo Trevisani "Brazil Legislators Bear Down on Internet Bill" *The Wall Street Journal* (online ed, New York, 13 November 2013).

72 Gordon M Goldstein "The End of the Internet?" *The Atlantic* (online ed, Washington DC, July/August 2014).

73 Council of Europe Convention on Cybercrime ETS 185 (opened for signature 23 November 2001, entered into force 1 July 2004).

computer data, searches of stored computer data and interception of traffic (metadata) and content data.

6.124 As at October 2016, the Budapest Convention had been ratified by 49 States (including Australia, the United Kingdom, Canada and the United States) and signed by an additional six States. New Zealand is not a signatory to the Convention. However, Part V of the Commonwealth Scheme for Mutual Assistance in Criminal Matters (the Harare Scheme),[74] of which New Zealand is a member, and the associated Model Legislation were drafted to give effect to Chapter III of the Convention. Therefore, while New Zealand is not legally bound by the Convention it has made a non-legally binding commitment to work towards compliance.[75]

6.125 At present, New Zealand's main mechanism for complying with Chapter III of the Convention is the Mutual Assistance in Criminal Matters Act 1992. The Law Commission recently reviewed that Act and made several recommendations designed to improve compliance with Chapter III of the Convention.[76] This included a proposal that the Act should clarify that foreign countries may request New Zealand authorities to obtain a production order on their behalf.[77] The Commission also proposed that there should be scope to use bilateral agreements to streamline the New Zealand process of approving and responding to such requests.[78] If New Zealand ratified the Budapest Convention then it would have access to similar mechanisms for facilitating access to stored data that are available in other member countries.

6.126 In addition to ratifying the Budapest Convention, the United States and the United Kingdom have reportedly begun negotiations to enter an agreement to allow each of their domestic law enforcement agencies to issue warrants directly to communication

---

74 Scheme Relating to Mutual Assistance in Criminal Matters within the Commonwealth including amendments made by Law Ministers in April 1990, November 2002, October 2005 and July 2011.

75 Not only is New Zealand a party to the Harare Scheme, it also developed an Action Plan to Fight Cybercrime in 2011 with the Quintet Commonwealth countries (Canada, the United Kingdom, the United States, Australia and New Zealand). The Action Plan concluded that all Quintet countries should take steps to become parties to the Budapest Convention.

76 Law Commission *Extradition and Mutual Assistance in Criminal Matters* (NZLC IP37, 2014) [EMA Issues Paper] at ch 17 generally and at [17.38]–[17.63]; and Law Commission *Modernising New Zealand's Extradition and Mutual Assistance Laws* (NZLC R137, 2016) [EMA Report] at ch 17 (which contains a draft Bill). The Government has accepted the Commission's recommendation that the Mutual Assistance in Criminal Matters Act 1992 should be replaced by new legislation and is currently considering the content of the draft Bill.

77 EMA Issues Paper, above n 76, at [17.38]–[17.43]; and EMA Report, above n 76, at 229 (cl 35(1)(a) of the draft Bill).

78 EMA Issues Paper, above n 76, at [17.108]; and EMA Report, above n 76, at 229 (cl 35(1)(b) of the draft Bill).

service providers in the other country to intercept communications or supply stored data for law enforcement purposes.[79]

6.127 This type of agreement would bypass the request and approval process required under the Mutual Assistance in Criminal Matters Act 1992 and the need to obtain a production order under the Search and Surveillance Act. This would save time and would not present any conflict with the 1992 Act because that Act specifically states that it is not a code for international assistance in criminal matters.[80] Such an agreement would, however, involve sacrificing a degree of sovereignty and control over the protection of individuals' privacy in New Zealand. Whether that sacrifice would be warranted is a matter of international relations and is outside the scope of this review.

Q29 Should the Act be amended to facilitate access to evidential material stored overseas?

## ASSISTANCE TO ACCESS COMPUTERS AND DEVICES

6.128 The Act empowers a person exercising a search power in respect of data held in a computer system or other data storage device to require a person to provide access information and other information or assistance that is reasonable and necessary to allow access to the data.[81] While the section is broadly drafted, it is usually used to require people to provide passwords or encryption keys. It is an offence to fail, without reasonable excuse, to assist when requested to do so. A conviction makes a person liable to imprisonment for a term not exceeding 3 months.[82]

6.129 Two issues arise in respect of this provision:

- whether the privilege against self-incrimination operates effectively in respect of this power; and
- whether the level of penalty for failing to comply with a request under this section is adequate.

---

79 Ellen Nakashima and Andrea Peterson "The British Want to Come to America – with Wiretap Orders and Search Warrants" *The Washington Post* (online ed, Washington DC, 4 February 2016); and Jennifer Daskal "A New UK–US Data Sharing Agreement: A Tremendous Opportunity, If Done Right" (8 February 2016) Just Security <www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/>.

80 Mutual Assistance in Criminal Matters Act 1992, s 5. The Law Commission recommended a similar provision in cl 10 of the draft Bill. See the EMA Report, above n 76, at 218.

81 Search and Surveillance Act 2012, s 130(1).

82 Section 178.

6.130 The first issue is discussed in detail in Chapter 8.

## Penalty for failure to assist

6.131 Enforcement agencies have told us that the current penalty for failing to comply with a request under section 130 is not high enough to motivate compliance in some cases. Suspects will weigh up the possibility of a maximum term of three months' imprisonment against the often much higher penalty they may face if the enforcement agency accesses the evidential material on their computer or electronic device. Often a rational decision is made to refuse to comply with the request for assistance.

6.132 One option is for the punishment to expressly provide for a fine as an alternative to imprisonment.[83] It has been suggested that a fine might provide more motivation to comply with the request than a jail term. Different types of penalty will motivate different types of offenders. For some, the prospect of a short term of imprisonment may not be as intimidating as for others. This may be particularly relevant where financial crimes are being investigated and successful prosecution may lead to the offender losing significant sums of money obtained.

6.133 If the offence is amended to expressly include a fine, there is a question as to the amount of that fine. We note that the offence of resisting a search under the Serious Fraud Office Act 1990 makes a person liable on conviction to either imprisonment for a term not exceeding three months or to a fine not exceeding $5,000.[84] Under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, the offences of obstructing an Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) supervisor and of providing false or misleading information to an AML/CFT supervisor carry penalties of up to three months' imprisonment or a fine of up to $10,000 for an individual (or a fine of up to $50,000 for a body corporate).[85] In line with these other statutes, it may be that a maximum fine in the range of $5,000–$10,000 is appropriate for the offence of failing to comply with a request to assist a computer search under the Act.

---

[83] We note that, in theory, a court may already impose a fine. Section 39(1) of the Sentencing Act 2002 provides that a court may impose a fine instead of imprisonment where an enactment provides for imprisonment but does not prescribe a fine. However, we do not know how often a fine has been imposed for failing to comply with a request under section 130, if at all.

[84] Serious Fraud Office Act 1990, s 47.

[85] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, ss 102, 103 and 105.

6.134 Of course another option would be to increase the maximum term of imprisonment. However, we do not currently favour that option because the length of imprisonment for failing to assist would not be equivalent to the level of penalty for the offence under investigation. Any increase would therefore be unlikely to provide any additional motivation to comply with the request.

Q30 Should the penalty for failing to provide access assistance be amended (for example, to explicitly provide for a fine as an alternative to imprisonment)?

# Chapter 7 – Warrantless powers

## INTRODUCTION

7.1 In New Zealand and in many other jurisdictions, warrantless powers have long been available for police officers to enter and search premises for law enforcement purposes in certain exceptional circumstances, where the public interest in swift police action outweighs the personal and privacy interests at stake. New Zealand Police also have warrantless powers under the Search and Surveillance Act 2012 (the Act) to search people in specified circumstances.

7.2 In the 2014/15 reporting year, Police exercised warrantless search powers on 7,048 occasions; and 3,866 people were charged in criminal proceedings where the collection of evidential material relevant to those proceedings was significantly assisted by the exercise of a warrantless search power.[1]

7.3 This chapter outlines the powers Police may exercise without warrant to enter and search places, vehicles and things under the Act. We describe the current scope of those warrantless powers, identify some issues that have arisen from the operation of the Act's provisions in practice and suggest some possible amendments.

7.4 A number of issues arise in relation to the operation of warrantless search powers under the Act, which we consider below:

- whether the thresholds for exercising warrantless powers are realistic to apply in practice;
- whether the warrantless powers should be exercisable only where a search warrant cannot be readily obtained and, if so, whether the Act should state that explicitly;
- whether searches of mobile electronic devices should always require a warrant; and
- whether the Act should provide a new power to enter a property without a warrant when an electronic monitoring device has been tampered with.

[1] New Zealand Police *Annual Report 2014/15* at 149.

## OVERVIEW OF THE WARRANTLESS POWERS REGIME

7.5 In its 2007 Report, *Search and Surveillance Powers*, the Law Commission identified various public interests that justify exercising warrantless powers, including: apprehending an offender who is a flight risk or who is unlawfully at large; preventing the imminent loss of or damage to evidential material; and averting an immediate risk to the life or safety of a person or serious damage to property.[2]

7.6 Prior to the enactment of the Act, warrantless powers for law enforcement purposes were found in various statutes and the common law. The Act codifies the existence and scope of those powers.

7.7 There is a range of warrantless powers available to Police under the Act. Broadly speaking, the purpose of the powers can be separated into five categories:

- warrantless powers of entry and search to preserve evidence;[3]
- warrantless powers of entry and search to make an arrest;[4]
- warrantless powers of entry to protect life and property;[5]
- warrantless powers to search for evidence of specific offences;[6] and
- warrantless powers to search places incidental to arrest or detention.[7]

7.8 For example, a police officer may enter and search a place without a warrant to find evidential material relating to serious offending if they have reasonable grounds to believe that the evidential material will otherwise be lost.[8] Police can also enter and search a place or vehicle without a warrant to arrest a person unlawfully at large.[9]

---

2 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.90].

3 For example, ss 8, 15, 16, 17, 25, 83, 84 and 88 of the Search and Surveillance Act 2012.

4 For example, ss 7, 8 and 9.

5 For example, ss 11, 14, 85 and 88.

6 For example, ss 18, 19, 20, 21, 22, 27, 28 and 29.

7 For example, s 11.

8 Section 15. Examples of cases that have considered the application of this section include *R v Lucas* [2015] NZHC 1944 and *Alamoti v R* [2016] NZCA 402.

9 Section 7. "Unlawfully at large" is defined in s 3 of the Act.

## THRESHOLDS FOR EXERCISING WARRANTLESS POWERS

### The thresholds in practice

7.9 During our preliminary consultation, we were told that warrantless powers can be difficult for police officers to apply in practice. We understand this stems from the wide variety of circumstances in which warrantless powers can be exercised and the need to remember the various threshold requirements applicable in each case. We are also aware of concern in some quarters that Police sometimes use warrantless powers too readily (for example, by misapplying the "reasonable grounds to believe" threshold where that is required before a particular search may be conducted).

7.10 These are operational issues and not ones that can be easily addressed by amending the legislation. An appropriate response is likely to involve further education and training for Police (for instance, on how to apply the various thresholds that need to be met before exercising the different warrantless powers). However, as we discuss below, it is possible that expressly recognising a preference for warrants over the use of warrantless powers in the Act would also help to reinforce the exceptional nature of warrantless powers.

7.11 A related issue raised during our preliminary consultation is that it can be difficult—in exigent circumstances—for enforcement officers to satisfy themselves that all of the preconditions for exercising a warrantless power are met. For example, we understand the application of section 8 of the Act can be problematic in practice.

7.12 Section 8 permits a police officer to enter a place or vehicle without a warrant to search for and arrest a person the officer suspects has committed an offence. In order to exercise this power, the officer must have reasonable grounds to suspect the person has committed an offence, reasonable grounds to believe the person is there, and reasonable grounds to believe that, if entry is not effected immediately, the person will leave the location to avoid arrest (or that evidential material relating to the offence will be destroyed, concealed, altered or damaged).

7.13 We were told it can be extremely difficult to satisfy all the preconditions for the exercise of this power. For example, it may be difficult (if not impossible) for a police officer to forecast another person's intentions: an officer might believe a person is going to leave an address, but may not know whether the person is leaving for the purpose of avoiding arrest (as opposed to some other purpose).

7.14 We have not analysed this issue in depth for the purposes of this chapter. However, we invite comments from submitters on whether the preconditions for the exercise of warrantless powers achieve the intended purpose and are realistic to apply in exigent circumstances.

Q31 Do the preconditions for the exercise of warrantless powers achieve the intended purpose and are they realistic to apply in urgent circumstances?

## Expressly limiting the use of warrantless powers to situations of urgency

7.15 In this section, we discuss the general question whether the Act should expressly limit the use of warrantless powers to situations where it is not practicable to obtain a warrant.

7.16 In 1993, the Court of Appeal held in *R v Laugalis*[10] that a search conducted pursuant to a warrantless statutory power (in that case, section 18(2) of the Misuse of Drugs Act 1975[11]) was unreasonable where there were no urgent circumstances and where a warrant could have been applied for. In that case, there was no reason for the police officer not to have applied for a warrant: the vehicle that was searched was being held in police custody. The Court said:[12]

> Although the power to search without warrant is not circumscribed by the [Misuse of Drugs Act], its reasonable exercise requires that it be resorted to only where that is reasonably necessary. … It is of particular importance where the drugs are believed to be in a motor vehicle. It would be absurd to require the police to obtain a warrant if in the meantime the vehicle could simply be driven away. But where there is no risk of that, no urgency, resort to the power is unnecessary and can in our opinion be unreasonable.

7.17 The Court acknowledged that its approach effectively wrote into section 18(2) "a restriction that the legislature has not thought appropriate to enact".[13] However, the Court reasoned that if its approach were not taken, section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA)—which guarantees the right to be secure against unreasonable search or seizure—would "[lose] much of its force".[14]

---

10 *R v Laugalis* (1993) 10 CRNZ 350 (CA).

11 Section 18(2) of the Misuse of Drugs Act 1975 provided that where a member of the Police had reasonable grounds for believing there was a specified controlled drug in or on any building, aircraft, ship, hovercraft, carriage, vehicle, premises or place, and that an offence against the Act had been or was suspected of having been committed, then there was a warrantless power to enter and search the place and any person found there.

12 *R v Laugalis*, above n 10, at 355–356.

13 At 356.

14 At 356.

7.18 The exact principle established by *Laugalis* was the subject of some debate. Some argued that the case introduced an additional prerequisite for the lawful exercise of the section 18(2) power: in other words, the use of that power would only be lawful if the circumstances were urgent and a warrant could not readily be obtained.[15] Others saw the case as standing for the more limited proposition that a search conducted pursuant to a warrantless power may be lawful yet unreasonable (under section 21 of NZBORA) where a warrant could have been readily obtained.

7.19 The courts preferred the latter view,[16] while also emphasising the need to have regard to the practicalities of policing in urgent situations. This includes consideration of whether a property can be kept under surveillance and evaluation of the resources available to officers at the time of assessing whether the situation faced made it reasonable to invoke a warrantless power.[17]

7.20 When the Law Commission prepared its 2007 Report, it considered whether the warrantless power provided in section 18(2) of the Misuse of Drugs Act should be amended to reflect the *Laugalis* decision. It recommended including a specific statutory provision that proscribes the use of the warrantless power unless the police officer exercising the power believes on reasonable grounds that it is not practicable to obtain a warrant.[18] This recommendation was carried through into what is now section 20 of the Search and Surveillance Act (which re-enacts, in modified form, section 18(2) of the Misuse of Drugs Act).

7.21 Section 20 provides:

> A constable may enter and search a place or vehicle without a warrant if he or she has reasonable grounds—

---

15 See for example the submission recorded in *R v Dobson* [2008] NZCA 359 at [12].

16 See *R v Smith* (1996) 13 CRNZ 481 (CA) at 485; *R v H* [1994] 2 NZLR 143 (CA) at 148; *R v Kingston* CA407/01, 18 March 2002 at [12]. *Laugalis* has sometimes been described as endorsing a "warrant preference approach": that is, it is "best practice" for powers of search and entry to be exercised pursuant to a warrant, even where a warrantless power is available: *Kalekale v R* [2016] NZCA 259 at [44]; *F v R* [2014] NZCA 313 at [46].

17 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [24]. See also *R v T* [2008] NZCA 99 at [16]; *R v Dobson*, above n 15, at [38]; and *Hughes v R* [2011] NZCA 661 at [25]. Cases decided both before and after the enactment of the Search and Surveillance Act 2012 have not limited the application of the *Laugalis* principle to warrantless searches of places and vehicles in respect of certain Misuse of Drugs Act offences (that is, s 18(2) of the Misuse of Drugs Act 1975 and s 20 of the Search and the Surveillance Act 2012). See *R v Williams* at [24]; *R v H*, above n 16, at 148; *Gillies v R* [2016] NZCA 289 (in relation to s 28 of the Search and Surveillance Act 2012); and *Kalekale v R*, above n 16 (in relation to s 15 of the Act).

18 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.65].

(a) to believe that it is not practicable to obtain a warrant and that in or on the place or vehicle there is—

(i) a controlled drug …

(b) to suspect that in or on the place or vehicle an offence against the Misuse of Drugs Act 1975 has been committed, or is being committed, or is about to be committed, in respect of that controlled drug or precursor substance; and

(c) to believe that, if the entry and search is not carried out immediately, evidential material relating to the suspected offence will be destroyed, concealed, altered, or damaged.

7.22 Section 20 is currently the only section in the Act that explicitly states that a warrantless search may only be conducted if there are reasonable grounds to believe it is not practicable to obtain a search warrant.[19]

7.23 When the Search and Surveillance Bill was going through the House, there was no discussion as to whether such a requirement should also apply to the other warrantless search powers. The Law Commission's 2007 Report did, however, consider whether the requirement should extend to the warrantless powers conferred on Police when offending against the Arms Act 1983 is suspected.[20] The Commission did not think there would be any advantage in requiring Police to believe a warrant could not readily be obtained before exercising those powers: given the immediate threat to safety that firearms pose, it was most unlikely to be practicable for a warrant to be obtained.[21]

7.24 We note that since the enactment of the Search and Surveillance Act, the courts have appeared to accept the proposition that the lawful exercise of *any* warrantless statutory power can be unreasonable where a warrant could have been readily obtained.[22]

7.25 We are interested in hearing views as to whether the use of all warrantless search powers under the Act should be limited to situations where it is not practicable to obtain a warrant.

---

19 We note that the wording of s 20(a) gives greater prominence to the *Laugalis* principle than it was given by the courts prior to the Act's enactment. As noted above, the courts accepted that a search conducted pursuant to a warrantless power could be lawful, but unreasonable, if there was no urgency and Police could have obtained a search warrant. But they did not interpret *Laugalis* as importing an additional requirement that needed to be satisfied *before* a warrantless search could be lawfully exercised: see in particular *R v Smith*, above n 16, at 485.

20 This is now contained in s 18 of the Search and Surveillance Act 2012.

21 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.66]–[5.67]. The Commission came to the same conclusion in relation to the warrantless power to enter a place to arrest a person unlawfully at large: at [5.25].

22 See *Gillies v R*, above n 17; and *Kalekale v R*, above n 16.

7.26 We note that limiting the use of all warrantless search powers in this way is arguably unnecessary. The underlying rationale for having warrantless powers is to allow enforcement officers to respond to urgent situations. This is already reflected in the statutory preconditions for the exercise of most of the warrantless powers. For example, section 8 of the Act permits the warrantless entry and search of a place or vehicle to arrest a person suspected of having committed an offence. The constable needs to have reasonable grounds to believe that, if entry is not effected immediately, the person will flee to avoid arrest or evidential material will be lost, altered or damaged.[23] Where that requirement is satisfied, it is difficult to imagine a situation where it would nonetheless be practicable for the constable to obtain a warrant.

7.27 On the other hand, expressly limiting the use of warrantless powers to situations where it is not practicable to obtain a warrant may reinforce the importance of using warrantless powers in exceptional circumstances only. Because warrantless powers are exercised without pre-authorisation by an issuing officer, it may be particularly important to underscore their exceptional nature to enforcement officers.

7.28 A related point is that requiring enforcement officers to be satisfied that it is not practicable to obtain a warrant would promote proactive protection of privacy interests. Without such a requirement, the reasonableness of using a warrantless power is only determined by a court *after* the power has been exercised (when considering a potential breach of section 21 of NZBORA), and only if the conduct is challenged.

Q32 Should the Act expressly limit the use of warrantless powers to situations where it is not practicable to obtain a warrant?

## WARRANTLESS SEARCHES OF ELECTRONIC DEVICES

7.29 A police officer conducting a warrantless search will sometimes encounter an electronic device in the place or vehicle searched or carried by the person searched. Currently, the law allows the person conducting the search to use reasonable measures to access a computer system or data storage device if intangible material that is the subject of the search may be on that device.[24] Often electronic devices such as smart phones and tablets are searched under warrantless powers because they are particularly mobile and there is a greater risk of evidence contained on them being lost, altered or

[23] Search and Surveillance Act 2012, s 8(2)(c).

[24] Sections 110(h) and 125(1)(l).

destroyed. However, in theory, warrantless powers would also apply to searches of less mobile electronic devices, such as personal computers, if the thresholds for the exercise of the power are met.

7.30 Prior to the advent of smart phones, the information that could be discovered during a warrantless search of an electronic device was generally fairly limited. However, as we discussed in Chapter 6, searches of electronic devices may now reveal significantly more information. The question for this review is whether the level of privacy invasion likely to be involved in a search of an electronic device is such that a warrant should always be obtained beforehand.

7.31 There have been a number of recent cases both overseas and in New Zealand that have considered this issue.

### *Riley v California*

7.32 In 2009, in the United States case of *Riley v California*, Mr Riley was stopped by Police for suspected traffic offences.[25] In accordance with police department policy, his car was impounded and subjected to a warrantless search. Two handguns were found, which were linked to a prior shooting. Upon arresting Mr Riley for that offence, Police confiscated and searched his smart phone without a warrant. Data from the phone was used in evidence in the trial at which Mr Riley was convicted.

7.33 Mr Riley argued that the warrantless search of his phone was an unacceptable intrusion on his privacy. The State of California argued that the search was required for safety reasons and to prevent the destruction of evidence. The question for the United States Supreme Court's consideration was whether Police could, without a warrant, search data on a cell phone seized from an individual who has been arrested.

7.34 It held that, except in extreme circumstances (for example, to prevent the imminent destruction of evidence, to pursue a fleeing suspect or to assist a person who was threatened with imminent injury), a search of a cell phone must always be done with a warrant:[26]

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," … The fact that technology now allows an individual to carry such information in his hand does not make the information any

---

25 *Riley v California* 573 US 1 (2014).

26 At 28.

> less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident [sic] to an arrest is accordingly simple – get a warrant.

### *R v Fearon*

7.35 In a 2014 case in Canada, Mr Fearon was arrested following an armed robbery of a jewellery seller at a Toronto market.[27] Following arrest, a pat-down search revealed his cell phone, which was searched both then and later at the police station. Incriminating text messages and photographs were found on the phone. The issue that came before the Supreme Court of Canada for consideration was the scope of the circumstances in which a warrantless search of a cell phone of an arrested person may be conducted.

7.36 The majority of the Court (four judges out of seven) recognised the important privacy interests implicated by searches of digital devices, but found that not every search of a cell phone is inevitably a significant intrusion on privacy. It held that cell phones may be searched without warrant following a lawful arrest under a common law power, but the potential for a significant invasion of privacy requires some modification to the standard rules. Four specific conditions must be met:

- the arrest must be lawful;
- the search must be truly incidental to the arrest – that is, it must be done promptly upon arrest and must effectively serve law enforcement purposes (protecting Police, the accused or the public; preserving evidence; or discovering evidence if the investigation will be stymied or significantly hampered without the ability to promptly conduct the search);
- the nature and extent of the search must be tailored to its purpose – in practice this means that generally only recently sent or drafted emails, texts, photos and the call log will be available; and
- Police must take detailed notes of what they have examined on the device and how they examined it.

7.37 The three dissenting judges placed a greater emphasis on preventing invasions of privacy and treated cell phones as unique sources of evidence. They thought that a warrant must be obtained before the content of a seized cell phone may be searched,

---

[27] *R v Fearon* 2014 SCC 77, [2014] 3 SCR 621.

except in exigent circumstances. They thought that the modifications proposed by the majority would generate problems of impracticality, police uncertainty and increased after-the-fact litigation. It would also require enforcement officers to determine whether law enforcement objectives outweighed the intrusion into privacy, despite their inherent conflict of interest in answering that question. And where their assessment is wrong, the subsequent exclusion of evidence would not be an adequate remedy for the initial privacy violation.

### *Dotcom v Attorney-General*

7.38 In this 2014 case, the New Zealand Supreme Court assessed the privacy interests in electronic devices in the context of considering the validity of a mutual assistance search warrant, which authorised searches of (amongst other things):[28]

> all digital devices, including electronic devices capable of storing and/or processing data in digital form, including, but not limited to … mobile telephones …

7.39 The Court found that computers (including smart phones) raise special privacy concerns because of the nature and extent of the information they hold and that the potential for invasions of privacy is high.[29] It held that:[30]

> … for a search of any computer to be reasonable, a mutual assistance warrant must give specific authorisation for the computer to be searched in order to identify and seize the data that it is believed is evidence of commission of an offence.

### *S v R*

7.40 In this very recent decision, the appellant challenged his conviction for importing drugs on the basis that the evidence obtained from his iPhones by New Zealand Customs Service officers as he entered the country was obtained by an unlawful and unreasonable search and was therefore inadmissible.[31] In searching the contents of the iPhones, Customs officers relied on the broad powers in section 151 of the Customs

---

28 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [87]. This case concerned the validity of search warrants that were executed by Police in 2012 at premises associated with Mr Kim Dotcom and Mr Bram van der Kolk. The United States has sought the extradition of these individuals to face trial on charges of racketeering, copyright infringement and money laundering. The warrants were held to be invalid in the High Court, but the Court of Appeal subsequently overturned that decision and concluded the warrants were valid. The Court of Appeal's decision was upheld by a majority of the Supreme Court.

29 At [191].

30 At [192].

31 *S v R* [2016] NZCA 448.

and Excise Act 1996 to examine or analyse goods that are subject to the control of Customs.

7.41 The appellant argued, relying on the remarks in *Dotcom v Attorney-General* about the special privacy concerns associated with computers, that:[32]

> Customs should not be entitled to treat every occasion when a person returns from overseas as a fortuitous opportunity to engage in highly invasive data collection when this would not be permitted in any other circumstances. The conduct of warrantless searches is not subject to judicial oversight or other statutory control with significant potential for serious abuse of such a power.

7.42 The Court of Appeal held that the search power in section 151 unambiguously permits iPhones to be searched as goods and was satisfied that there was no scope to read down the explicit language of that section to have regard to the privacy interests of the owner of the iPhones.[33] It said that if Parliament had intended a warrant to be required for searches of electronic devices, it would have said so.[34]

7.43 We note that the Government has recently announced proposals to amend the Customs and Excise Act.[35] Currently, there is no threshold that must be satisfied before a Customs officer can exercise the power to examine goods under section 151. However, as part of the proposals Cabinet agreed in principle that Customs officers should not be able to examine or search data stored on, or accessible from, electronic devices without appropriate statutory thresholds being met. Cabinet noted that compliance with NZBORA would likely be satisfied by a two-threshold test requiring reasonable suspicion of criminal offending and reasonable belief that the device contains evidential material.[36]

### *Analysis*

7.44 We have identified a number of options for how the Act should deal with searches of electronic devices:

- retaining the status quo;
- requiring a warrant to be obtained for all searches of electronic devices; or

---

32 *S v R*, above n 31, st [19].

33 At [32] and [44].

34 At [45].

35 Cabinet Minute "Customs and Excise Act Review: Powers, Obligations and Regulated Goods" (2016) CAB-16MIN-0015.01.

36 As above.

- a middle option – permitting the device to be held while a warrant is obtained.

7.45 In addition to these options (discussed below), it should be noted that two of the options for reform identified in Chapter 6 (which seek to address the risk of seeing too much irrelevant material during an electronic search) could also be relevant to searches of all electronic devices. Those two options were a requirement to document search procedures[37] and a statutory duty to take steps to avoid seeing privileged or irrelevant material.[38]

### Status quo

7.46 Currently, the risk of unreasonable searches of electronic devices is primarily managed through section 30 of the Evidence Act 2006 and section 21 of NZBORA.[39] Where the prosecution seeks to adduce evidence from a warrantless search of an electronic device in criminal proceedings, the defendant may challenge the admissibility of the evidence under section 30 on the basis that it was improperly obtained. The grounds for that challenge would be that the search was unreasonable under section 21 because a warrant was not obtained in circumstances where it could have been. This potential for exclusion of evidence provides motivation for the person carrying out a search to obtain a warrant, if it is reasonably practicable in the circumstances.

7.47 The advantage of retaining the status quo is that it retains the flexibility for enforcement officers to search electronic devices under warrantless powers when the appropriate thresholds, if any, for exercising those powers are met. It would be consistent with the majority finding in *R v Fearon* that searches of electronic devices are not inevitably a significant invasion of privacy. For example, if the enforcement officer has grounds to believe that a suspect had an accomplice whose name was known to the officer, it may be reasonable to search the contact list or very recent texts on a smart phone without a warrant on the basis that the information would likely be deleted if it was not obtained immediately.

7.48 The main disadvantage of this option is that section 30 can only offer a remedy after the search has occurred, and only if criminal proceedings eventuate. While the risk of

---

37 See paragraphs [6.42]–[6.44].

38 See paragraphs [6.52]–[6.56].

39 See for example *Hoete v R* [2013] NZCA 432, (2013) 26 CRNZ 429; *McLean v R* [2015] NZCA 101; and *R v Lucas* [2015] NZHC 1944.

having evidence subsequently ruled inadmissible provides some motivation for enforcement officers to ensure searches are reasonable, that may provide a fairly weak protection of privacy interests. Also, it could be argued (as it was by the minority in *R v Fearon*) that enforcement officers have a conflict of interest when assessing whether a search of an electronic device without a warrant is unreasonable.

7.49 It should also be noted that, even if a court finds that evidence was improperly obtained under the Evidence Act, the evidence may still be admissible if the court determines that exclusion of the evidence is disproportionate to the impropriety.[40]

### Warrants for all searches of electronic devices

7.50 The Act could specify that all searches of electronic devices must be authorised by a warrant. That would mean that in all cases where an officer wishes to search an electronic device, a search warrant would first have to be obtained.

7.51 The advantage of this option is the independent assessment of the exercise of the power by an issuing officer. That assessment would provide some assurance that the search is being conducted within the legal limitations.

7.52 However, the disadvantage is that it can take a number of hours to obtain a search warrant. In the meantime, the evidence on the electronic device could be deleted, amended or otherwise destroyed. Also, the device itself may no longer be able to be located by the time the warrant is obtained.

7.53 A modified version of this option would permit an exception to the requirement in exigent circumstances (for example, where there is a risk of the imminent destruction of evidence). This was the position adopted by the Court in *Riley v California*. However, it could be argued that an ability to dispense with the requirement for a warrant in exigent circumstances provides little extra protection beyond what the current thresholds for warrantless searches provide. As we described in the previous section of this chapter, the thresholds for warrantless searches are generally designed to apply only in exigent circumstances because that is the underlying rationale for searches without a warrant.

---

[40] Evidence Act 2006, s 30(2)(b).

### The middle option – hold the device while a warrant is obtained

7.54 Under this option, the Act could be amended to both:

- require a warrant to be obtained before conducting a search of an electronic device (as described above); and
- provide a power to seize (but not search) the device in order to preserve the evidence while a search warrant is obtained.

7.55 We note that an ability to preserve evidence pending an application for a warrant would not be a new concept under the Act. Section 117 permits enforcement officers to secure a place, vehicle or other thing pending determination of a search warrant application.

7.56 This option retains the advantage of the previous option (independent oversight by an issuing officer), but overcomes the disadvantage. The enforcement officer could be required to disconnect the device from the Internet so that the data on it cannot be remotely updated, amended or deleted (for example, by switching it to "flight mode"), place the device in a sealed bag and retain it in secure storage at the police station. The Act would need to provide a time limit within which the device is either retained for search under a warrant or returned to its owner.

7.57 The disadvantage (depending on the circumstances) of this option is that the owner does not have possession of the device pending the warrant being obtained. That would need to be weighed up against the advantages of obtaining a warrant.

Q33 Should warrants always be required for searches of electronic devices? If so, should there be an exception for urgent circumstances and/or a power to seize the device while a warrant is obtained?

## POLICE POWERS OF ENTRY – TAMPERING WITH ELECTRONIC MONITORING DEVICES

7.58 Currently, Police do not have an express power to enter a property without a warrant when an alert is received suggesting an occupant subject to electronic monitoring may have tampered with his or her electronic monitoring device.

### *What is electronic monitoring and when is it used?*

7.59 Electronic monitoring is a where a tracking device is attached to a person's ankle to monitor their compliance with the conditions of a sentence or order imposed by a court.[41] The tracking device must be worn 24 hours a day, seven days a week for the duration of the sentence or order. A monitoring unit is also installed at the person's address and, in some cases, their place of employment.

7.60 There are two types of electronic monitoring – Radio Frequency (RF) and Global Positioning System (GPS). RF is mainly used for community detention to monitor the offender at their detention address.[42] GPS is used to monitor the location of a person whether at home or away from their address – for example, under sentences of home detention,[43] extended supervision orders[44] or bail orders.[45] It can also be used to monitor compliance with a special condition following an offender's release from prison or an intensive supervision order made in respect of a young person.[46]

7.61 The monitoring system will receive an electronic alert if something unusual happens to the tracker, for example if a person tampers with it. However, alerts can occur for a number of reasons besides removal or deliberate interference: for example, if the tracker is accidentally knocked or submerged in water. When an alert occurs, the matter can often be resolved by a Corrections field officer or probation officer contacting the person and ascertaining what happened. In other cases, a police officer may be called. We understand that, more often than not, a person subject to electronic monitoring will come to their door if an officer is sent to their address to respond to a tamper alert. Access to the premises by Police is only required in those cases where the person does not come to the door, to check whether they have absconded.

7.62 The Department of Corrections told us that approximately 4,000 people are subject to electronic monitoring at any one time and tamper alerts frequently occur. It estimates there may be three cases per day in which access to the house by Police is required because the matter is not able to be resolved in other ways. Corrections emphasised

---

41 Department of Corrections "Electronic monitoring" <www.corrections.govt.nz>.

42 Sentencing Act 2002, s 69E(1)(e).

43 Section 80C(2)(d).

44 Parole Act 2002, ss 15 and 107K.

45 Bail Act 2000, s 30B.

46 Parole Act 2002, s 15 and Children, Young Persons, and Their Families Act 1989, s 296J(6).

that those cases tend to be higher risk cases, because low-risk cases are usually able to be resolved by other interventions.

### *Problem*

7.63 If Corrections receives an alert that a device has been tampered with and the device is inside the property of the person subject to electronic monitoring, there is no statutory authority for a police officer to enter the property without a warrant to check whether the person is inside.

7.64 Under the Act, a police officer can only enter and search a place without a warrant to locate a person if he or she:

- has reasonable grounds to suspect the person is unlawfully at large and to believe the person is at the property;[47] or
- has reasonable grounds to suspect the person has committed an offence, and to believe the person is at the property and may flee to avoid arrest if entry is not effected immediately.[48]

7.65 In circumstances where the police officer only has information that the electronic monitoring device has been tampered with and that the device is in the property, it will often be the case that neither of these two powers apply. The powers require the officer to have reasonable grounds to believe the person is at the property. Police are more likely to suspect that a person who has tampered with his or her electronic monitoring device has *left* the address.

7.66 We understand the absence of a warrantless power in these circumstances may hinder the ability of Police to effectively respond to tamper alerts. Because Police do not have an express power to enter the property, they cannot be sure if the person has absconded.[49] Without this information, Police may be reluctant to launch a full-scale search for the individual in the community.

---

47 Search and Surveillance Act 2012, s 7.

48 Section 8. The suspected offence must be punishable by imprisonment and one for which the individual can be arrested without warrant. Section 8(2)(c)(ii) also allows an officer to enter a place or vehicle without a warrant if they believe evidential material will be lost if entry is not effected immediately.

49 In theory, Police could obtain a search warrant under s 6 of the Act in order to lawfully enter the property on the basis that there are reasonable grounds to suspect an offence has been committed (for example, a suspected breach of the sentence condition or order that requires the person to be subject to electronic monitoring); and reasonable grounds to believe that

7.67 This issue recently arose in relation to a child sex offender who removed his electronic tracking device while subject to an extended supervision order. Police were notified that his device had been tampered with and was still inside the property, but they had no way of knowing whether he was still there or had fled. Because there did not appear to be any applicable warrantless power under the Act that would allow entry into the property in those circumstances, Police were unable to immediately enter and check whether he was present.[50]

### *Option for reform: a new warrantless power*

7.68 One possible solution is for a new section to be inserted into the Act,[51] conferring an explicit power on Police to enter a property without a warrant upon receiving information from Corrections that an electronic monitoring device has been tampered with and was last located inside the property. This new section would not require a constable to have reasonable grounds to believe that the person is present before entering the property. The threshold for the exercise of the power could be that there are reasonable grounds to suspect the electronic monitoring device has been tampered with and reasonable grounds to believe that it is in the property.

7.69 There is a strong public interest in apprehending offenders who are a flight risk. This is the policy justification for the warrantless power that permits Police to enter a property to apprehend an offender who may flee to avoid arrest.[52] If there is reason to suspect that a person has tampered with his or her electronic monitoring device and may have absconded from his or her monitored address, there is a similar public

---

evidential material in respect of the offence (such as a broken/abandoned electronic monitoring device) will be found on the property. However, the process of applying for and obtaining a warrant under s 6 may take too much time.

50 This incident was noted during a recent government inquiry into State sector agencies' management of another offender (who was convicted of rape and murder committed while being electronically monitored after his release from an eight-year term of imprisonment for child sex offending). The inquiry did not analyse whether Police could have lawfully used a warrantless power under the Act, but instead noted that the issue could be explored more fully in our review of the Act: see Mel Smith *Government Inquiry into Tony Douglas Robertson's Management Before and After his Release from Prison in 2013* (29 January 2016) at 6 and 64–65.

51 We suggest the new section is inserted into the Search and Surveillance Act (rather than under the legislation that governs the imposition of electronic monitoring, such as the Parole Act 2002 or Sentencing Act 2002) because this aligns with the original legislative intention to codify the existence and scope of Police warrantless powers that were previously scattered across different statutes.

52 Search and Surveillance Act 2012, s 8. See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.90].

interest in giving police officers the ability to respond in a timely and effective manner.

7.70 However, there is a risk that such a power could be used in a manner that unduly infringes on the privacy of persons subject to electronic monitoring (for example, if Police were to enter all properties, as a matter of course, where an alert is received). To avoid this, the Act could require a police officer to take reasonable steps to ascertain whether the person is at the address before entering the property. This could include, for example, knocking on the door and/or calling the person's phone so that they have an opportunity to present themselves voluntarily.

Q34 Should the Act allow Police to enter a property to search for a person subject to electronic monitoring without a warrant, if there are reasonable grounds to suspect the electronic monitoring device has been tampered with?

# Chapter 8 – Privilege

## INTRODUCTION

8.1 In this chapter we describe how privileged material in general is protected under the Search and Surveillance Act 2012 (the Act) and how the privilege against self-incrimination applies during the investigation phase. We identify where there may be gaps in the process and suggest options for strengthening the relationship between law enforcement and human rights values.

## BACKGROUND

### What is evidentiary privilege?

8.2 Almost any person can be compelled to give evidence in legal proceedings.[1] Privilege is the ability to withhold certain kinds of evidence (oral or written) in those proceedings. This ability is described as a 'privilege' because the person who owns the privilege must claim it to trigger its protective effect.

8.3 A successful claim gives the privilege owner the right to refuse to disclose the evidence, if they are asked to do so. It sometimes also confers the right to require that other people who were recipients of a privileged material or other persons who now possess that material do not disclose it either.[2]

8.4 There are several different privileges and no single public interest explains their existence. But each privilege reflects a value that is considered to outweigh the public interest in having all relevant evidence available for the proper functioning of the administration of justice.

8.5 Some privileges are based on the way in which our adversarial[3] legal system works, such as legal professional privilege,[4] the privilege against self-incrimination[5] or the

---

1 Evidence Act 2006, s 71. There are exceptions contained in s 73 (defendants and associated defendants) and s 74 (the Sovereign and certain other persons). "Proceeding" means a proceeding conducted by a court and any interlocutory or other application to a court connected with that proceeding; "Court" includes the Supreme Court, Court of Appeal, High Court and any District Court (which includes the Family and Youth Court): see the Evidence Act 2006, s 4.

2 Evidence Act 2006, s 53(4).

3 In adversarial systems, parties conduct investigations and then present the evidence to an independent fact finder, either a judge sitting alone or a jury. This contrasts with inquisitorial systems, where the judge has an investigative as well as adjudicative role and makes inquiries on his or her own initiative.

privilege that exists in relation to communications between parties or between a party and a mediator when trying to settle a dispute. The underlying rationale of other privileges is the social value in protecting certain relationships that require confidentiality to operate: for example, communications between a person and their minister, a doctor and their patient, or an informant and an enforcement agency.

8.6 Prior to 2006, privileges were either located in the common law or in statute law. For example, legal professional privilege was created and refined through a series of judicial decisions, whereas privilege in relation to communications by a patient with their doctor was determined by legislation.

8.7 The Evidence Act 2006 now provides for claims to all of these privileges in proceedings.[6] This is the first time in our legal history that a general statutory regime for such claims in proceedings was enacted.[7]

---

4 Legal professional privilege is the precursor to the current privileges for legal advice and for preparatory materials that now operate in proceedings and it has been retained for contexts other than proceedings. First, it protects confidential communications between a person and their legal adviser from disclosure, to ensure that free and frank advice is given and received; second, it protects some other information that is generated by each party while preparing for litigation from disclosure to the other side.

5 There are alternate explanations for the origins of the privilege against self-incrimination: the right not to be compelled to confess guilt, now reflected in s 25(d) of the New Zealand Bill of Rights Act 1990. One is nested in opposition in the late 17th century to the use of the ecclesiastical oath and Star Chamber inquisitions as methods of questioning. The other explanation focuses on the late 18th century development of the adversarial process – the concept of an independent fact finder hearing allegations and responses from equal opposing parties. The privilege was part of the rules of evidence designed to maintain this equality. For a summary, see Law Commission *The Privilege Against Self-Incrimination* (NZLC PP25, 1996) at [14]–[20].

6 It should be noted that the privilege against self-incrimination also applies beyond proceedings. It is also available where the request to supply specific information is made by a person exercising a statutory power or duty or by a police officer or other person holding a public office who is investigating a criminal or possible criminal offence: s 60(1) of the Evidence Act 2006.

7 The Evidence Act 2006 also provides two different judicial discretions (ss 69 and 70) that prevent disclosure of material that is confidential but for which privilege cannot be successfully claimed. These are not recognised by the Search and Surveillance Act 2012. There are discrete evidentiary privileges in other legislation that are not relevant in this context, since the Act does not recognise them in the investigation and collection of evidence phase. In its 2007 Report, the Commission recommended that the qualified protection provided by these sections should not be available when enforcement powers are exercised: Law Commission *Search and Surveillance Powers* (NZLC R97, 2007), recommendation 12.25.

## Current law

### *Privileges that apply in the process of search and surveillance*

8.8 In its 2007 Report, *Search and Surveillance Powers*, the Law Commission concluded that material for which a claim of privilege would be available at trial should also be protected from disclosure during the investigation and evidence collection phase. The Commission stated:[8]

> Codification of the procedure to be followed where the exercise of search and surveillance powers involves or could involve material that is subject to legal privilege (the three statutory areas of lawyer-client privilege, litigation privilege and privilege for settlement negotiations or mediation) is recommended. Where a claim of legal privilege arises, the recommendations are directed to facilitating the making of a claim, securing and isolating the material concerned, and ensuring that it is not examined for law enforcement purposes until the claim is resolved.
>
> Recommendations are made for the codification of a similar procedure where privileged communications with ministers of religion, medical practitioners, or registered clinical psychologists are or may be implicated by the exercise of a search or surveillance power. Similar procedures are also proposed in respect of material identifying journalistic sources that attracts qualified protection under the Evidence Act 2006.

8.9 The Commission also discussed the privilege against self-incrimination:[9]

> We see little to be gained by recommending, for general crime investigations, a statutory process that requires suspects or people who may be the subject of the investigation to produce documents that may incriminate themselves.

8.10 In deciding exactly what claims to privilege could be made, the Commission adopted the privileges as described in the Evidence Act. The policy reason for aligning privilege claims during the investigation and collection phase with those available at trial was to promote consistency. It was thought that a single regime would avoid the potential for a mismatch in the application of the principles.[10]

8.11 This approach was carried through to the Search and Surveillance Act.[11] Each privilege recognised in the evidence collection phase is described by reference to how

---

8 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [44]–[45].

9 At [10.31] when discussing the policy reasons for production orders. It needs to be noted that examination orders (which also raise issues in relation to self-incrimination) were not addressed in the Commission's Report.

10 At [12.8]–[12.10].

11 Search and Surveillance Act 2012, s 136. Given that the drafting of the privileges in the Evidence Act 2006 focuses on the trial phase, the descriptions of what is protected are not always a good fit for the investigation phase. For example, the limited protection from non-disclosure of a journalist's source in s 68 of the Evidence Act is expressed in terms of the compellability of that journalist to answer questions or produce a document. This presupposes a trial process has commenced. Similarly, informer privilege in s 64 of the Evidence Act protects an informant's identity only if they are not

it is described in the Evidence Act for the trial phase. This means that what is protected from disclosure is the same as if the privilege claim had been made at trial.

8.12 The nature of each privilege is briefly described below:

- **Privilege for communications with legal advisers:** This privilege protects communications (oral and written) between a person and their legal adviser that are intended to be confidential and are made during the course of and for the purpose of the giving or obtaining of legal services.[12]
- **Privilege for preparatory materials in proceedings:** This privilege protects communications or information if it is made, received, prepared or compiled for the dominant purpose of preparing for proceedings. It protects several kinds of communications that may arise in this context. First, it protects communications between either the legal adviser or the client and another person (such as an expert); second, it covers information compiled or prepared by the client or the legal adviser; and third, it also applies to information compiled or prepared by another person at the request of either the client or the legal adviser.[13]
- **Privilege for settlement negotiations or mediation:** This privilege protects communications between parties to a civil dispute or with a mediator, made in confidence for the purpose of attempting to settle or mediate the dispute. It also extends to confidential documents that parties prepare or cause to be prepared for the same purpose.[14]

---

being called as a prosecution witness to give evidence in relation to the information they supplied. However, it is not clear whether this has created problems in practice.

12 Evidence Act 2006, s 54. When it comes into force, the Evidence Amendment Act 2016 will clarify the privilege by adding s 54(1A): "The privilege applies to a person who requests professional legal services from a legal adviser whether or not the person actually obtains such services". That Act will come into force either on a date appointed by the Governor-General by Order in Council (and one or more orders may be made bringing different provisions into force on different dates) or on 1 July 2017, whichever is the earlier date: Evidence Amendment Act 2016, s 2. "Legal adviser" covers a New Zealand lawyer who holds a current practising certificate or a registered patent attorney or, in some situations, an overseas practitioner: s 5(1) of the Evidence Act 2006.

13 Section 56. See *Beckham v R* [2015] NZSC 98, [2016] 1 NZLR 505 and *Jeffries v Privacy Commissioner* [2010] NZSC 99, [2011] 1 NZLR 45 for examples of how the privilege operates.

14 Section 57. When the Evidence Amendment Act 2016 comes into force (see footnote 12 above), it will extend this privilege to plea discussions (those conducted in criminal proceedings).

- **Privilege for communications with ministers of religion:** This privilege protects communications made in confidence between a person and a minister of religion for the purpose of receiving religious or spiritual advice, benefit or comfort.[15]
- **Privilege in criminal proceedings for information obtained by medical practitioners and registered clinical psychologists:** This privilege protects communications with and information obtained by medical practitioners and registered clinical psychologists in the course of treating a person for drug dependency and any other condition or behaviour that may manifest itself in criminal conduct.[16]
- **Informer privilege:** This privilege protects information that would or is likely to disclose the identity of an informer, but only if they are not called by the prosecution to give evidence relating to the information that they supplied.[17]
- **Privilege against self-incrimination:** This privilege allows a person to refuse to provide specific information that would be likely to incriminate them under New Zealand law in relation to an offence punishable by a fine or imprisonment.[18] It applies to an oral response or written response. The privilege only applies in some situations (not in civil proceedings, for example) and can be removed by other statutes.[19] If it applies, the person cannot be prosecuted or penalised for refusing or failing to provide the information.
- **Limited protection for a journalist in relation to non-disclosure of a source:** There is also a limited protection for a journalist (or their employer) in relation to disclosure of the identity of a source or information enabling that identity to be

---

15 Evidence Act 2006, s 58.

16 Section 59. "Drug dependency" is defined by reference to "controlled drug", as defined in s 2(1) of the Misuse of Drugs Act 1975.

17 Section 64. An informer is defined as a person who "has supplied, gratuitously or for reward, information to an enforcement agency, or to a representative of an enforcement agency, concerning the possible or actual commission of an offence in circumstances in which the person has a reasonable expectation that his or her identity will not be disclosed".

18 Section 60. The situations are where a person is required to provide that information in the course of a proceeding or by a person exercising a statutory duty or power or by a police officer or other person holding a public office in the course of an investigation into a criminal offence or possible criminal offence: s 60(1)(a).

19 For example, s 27 of the Serious Fraud Office Act 1990 expressly removes the ability to claim the privilege.

discovered.[20] A successful claim provides relief from being compellable to answer questions or produce information that would disclose the source's identity. This is not an absolute privilege. It does not bar admission into evidence of material, as the other privileges do if their elements are satisfied and there are no grounds to disallow the privilege claim.[21] Limited protection means the court has discretion to determine that the protection does not apply. To lift the protection, the court must first be satisfied that the public interest in disclosure of the informant's identity outweighs any likely adverse effect of disclosure on the informant or another person. Second, it must be satisfied that the public interest in disclosure outweighs the public interest in the communication of facts and opinion to the public by the news media, and the ability of the news media to access sources of facts.[22]

### *How privileged material is protected*

8.13 If a claim for any of the privileges or the limited protection described above is upheld by a judge, the communication or information to which it applies is not admissible in any proceedings arising from or related to the execution of a search warrant, the exercise of warrantless search or surveillance powers or the carrying out of an examination order or production order. [23]

8.14 In terms of the relationship between the Evidence Act and the Search and Surveillance Act:

- the Evidence Act lays out the nature and breadth of each privilege (the elements necessary for a successful claim);

---

[20] Evidence Act 2006, s 68: "If a journalist has promised an informant not to disclose the informant's identity, neither the journalist nor his or her employer is compellable in a civil or criminal proceeding to answer any question or produce any document that would disclose the identity of the informant or enable that identity to be discovered".

[21] Except for the privilege against self-incrimination, a claim to privilege can be disallowed under s 67 of the Evidence Act 2006 if: there is a "prima facie case that the communication was made or received, or the information was compiled or prepared, for a dishonest purpose or to enable or aid anyone to commit or plan to commit what the person claiming the privilege knew, or reasonably should have known, to be an offence"; or if a judge is "of the opinion that evidence of the communication or information is necessary to enable the defendant in a criminal proceeding to present an effective defence".

[22] Section 68(2).

[23] Search and Surveillance Act 2012, s 148.

- the Search and Surveillance Act determines how a claim to privilege will be made and managed in the investigation and evidence collection phase;
- the Evidence Act determines whether the claim to privilege is successful; and
- the Search and Surveillance Act states what will happen to the material for which privilege has successfully been claimed, both in a practical sense and in terms of barring its use in later proceedings.

8.15 The regimes for managing claims to privilege differ depending on the type of warrant or power being exercised or the order being executed.

### Search warrants and other search powers

8.16 If a warrant authorises the search of materials held by a legal adviser relating to a client, the legal adviser (or their representative or a New Zealand Law Society appointee) must be present to represent the interests of the client. They must be given the ability to claim privilege on behalf of the client or to make an interim claim, if instructions have not been obtained from the client (the privilege owner).[24]

8.17 If the search involves professional material held by a minister of religion, medical practitioner or clinical psychologist, the process is similar. It can involve an appointee from the church or relevant professional body (if the professional or their representative is unavailable) and an interim claim if the professional cannot contact the parishioner, patient or client who owns the privilege.[25]

8.18 In other search contexts, if the person executing the search warrant or exercising a search power has reasonable grounds to believe that anything discovered in the search may be the subject of a privilege, he or she must provide the person who might be able to claim privilege with a reasonable opportunity to do so.[26] If it is not possible to identify or contact that person (or to contact their lawyer) within a reasonable period, the searcher can apply to the District Court to determine the privileged status of the thing discovered in the search.[27]

---

[24] Search and Surveillance Act 2012, s 143.

[25] Section 144.

[26] Section 145. For example, it was noted in *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523 at [84] that s 145 covers searches of a journalist's materials (even though it is not a privilege but a qualified protection). The High Court must determine this claim: s 136(3). *Hager* is discussed further at paragraphs [8.28]–[8.34] below.

[27] Section 145(2).

8.19 The Act sets out a number of interim steps that may be taken if a thing is unable to be immediately searched due to a claim of privilege. The person executing the warrant or exercising a search power may secure the thing (and make a forensic copy if it is intangible, such as computer data), and deliver it to the relevant court. The person must supply the lawyer or other person claiming privilege with a copy of or access to the secured thing. The person must also refrain from searching the thing unless there is no claim to privilege or it is withdrawn, or the search is in accordance with the directions of the court determining the claim of privilege.[28]

8.20 The Act makes it clear that a person cannot make a blanket claim of privilege for things that are seized or sought to be seized. The person must provide a particularised list in relation to things for which privilege is claimed. If it is not possible to do so, the claimant may apply to the court for directions or relief.[29]

8.21 A privilege claim in the context of a search warrant or search power allows the claimant to prevent the search of privileged material pending the claim being determined and if it is upheld. The claim also provides the basis for requiring the return of a copy of the communication or information, or access to it if it has already been seized, pending determination of the claim.[30]

### Production and examination orders

8.22 The privilege against self-incrimination can be claimed in support of a refusal to comply with a production order or an examination order.[31] Other claims to privilege can also provide the basis for that refusal.[32] The District Court can determine whether the claim is valid. A successful claim to privilege then justifies the refusal to produce the information or document sought or to answer the question.

---

28 Search and Surveillance Act 2012, s 146.

29 Section 147.

30 Section 142.

31 Section 138(2). A claim to the privilege against self-incrimination is only possible in relation to production and examination orders: ss 136(1)(g) and 138(1). It is not available in relation to surveillance or the execution of search warrants.

32 Section 139. The drafting of s 139(1) seems to assume that the person subject to the order must be the owner of the privilege, rather than claiming it in a representative capacity for another (unlike the search warrant provisions).

## Surveillance

8.23 Claims to privilege (except the privilege against self-incrimination) can be made in relation to surveillance authorised under the Act, whether or not that surveillance requires a surveillance device warrant.

8.24 There is a duty on the person undertaking surveillance to take all reasonable steps to prevent surveillance of privileged material and to destroy any record of such material unless that is impossible or impracticable to do without destroying non-privileged records.[33]

8.25 Once aware of the surveillance, the person claiming privilege can prevent (as far as it is reasonably practicable to do so) the surveillance of the privileged communication or information. If the claim is upheld, the person can require destruction of the record of the privileged communication or information, to the extent this can be achieved without destruction of any non-privileged material.[34]

8.26 The District Court can determine whether the privilege claim is valid. If it is, any evidence of the privileged communication or information recorded by the surveillance is not admissible as evidence – unless the privilege owner consents (in other words, waives the privilege) and the court agrees to admit it.[35]

### *Duty of candour*

8.27 Applications for a search warrant are made without notice to the party who might be affected by its issue. This is an exception to the general right under an adversarial system for the affected person to oppose an application. In light of this exception the common law imposes a duty of candour on the applicant. This is an obligation to make full disclosure of all facts relevant to the question whether the warrant should be issued.[36] Breaching that duty by failing to present the 'full picture' risks the process of issue being considered legally defective, the warrant invalid and the search unlawful.[37]

---

33 Search and Surveillance Act 2012, s 140(2).

34 Section 140(1).

35 Section 140(5).

36 Prior to the Act, the leading case recognising the duty of candour was *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA). In 2015, the Supreme Court in *Beckham v R*, above n 13, endorsed the ongoing relevance of the duty of candour. One of the warrants at issue (obtained in 2009 and so prior to the Act) sought call data from a public (monitored) phone in a prison and had knowingly included the telephone number of the lawyer for Mr Beckham on the list of material to

8.28 *Hager v Attorney-General*[38] provides an example of what can happen. That case involved the issue and execution of a "media warrant" – a search warrant involving a journalist.[39] Nicky Hager was an investigative journalist who authored *Dirty Politics*, a book published during the 2014 general election that alleged a "dirty tricks" campaign in support of the National Party by Cameron Slater (publisher of the "Whale Oil" blog).[40]

8.29 Mr Hager's allegations were based on information supplied by his confidential source, known by the nickname "Rawshark". In investigating whether Mr Slater's computer was illegally accessed by Rawshark to supply that information, New Zealand Police applied for a search warrant for Mr Hager's home.[41]

8.30 During the warrant's execution, Mr Hager claimed the right under section 68 of the Evidence Act to protect a source. Numerous electronic devices, storage media and paper documents were seized and a smart phone was cloned. The material was delivered to the High Court under the Act to determine the validity of the claim. However, this did not proceed because Mr Hager initiated proceedings to judicially review the lawfulness of the issuing of the warrant and to seek return of the material. One ground of invalidity relied upon was the protection of source identity.

8.31 The High Court rejected the Crown's argument that privilege need not be addressed in the warrant application and could instead be left to be managed by the procedures

---

be seized, without advising the court of this. The Crown accepted that the warrant application should have expressly addressed the question of calls attracting privilege and set out a process to deal with them. The Court ruled that the lack of candour in the application made the process of issue defective and rendered the warrant unlawful. This made the seizure of material unreasonable and in breach of s 21 of the New Zealand Bill of Rights Act 1990.

37 *R v McColl* (1999) 17 CRNZ 136 (CA) at 142–143, discussed in *Tranz Rail Ltd*, above n 36, at 788–798 and in *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [127], and referred to in *Hager v Attorney-General*, above n 26.

38 *Hager v Attorney-General*, above n 26.

39 'Journalist' is defined in s 68(5) of the Evidence Act 2006 as "a person who in the normal course of that person's work may be given information by an informant in the expectation that the information may be published in a news medium".

40 Nicky Hager *Dirty Politics: How Attack Politics is Poisoning New Zealand's Political Environment* (Craig Potton Publishing, Nelson, 2014).

41 The warrant was based on Mr Hager being considered an uncooperative witness rather than a suspect. The reason for this was the Court of Appeal's decision in *Dixon v R* [2014] NZCA 329, [2014] 3 NZLR 504. The effect of that decision was that, even if Mr Hager were found in possession of the material, as a matter of law the material could not be regarded as stolen because digital files were not "property". That decision was subsequently overturned in *Dixon v R* [2015] NZSC 147, [2016] 1 NZLR 678.

provided in the Search and Surveillance Act. It ruled that the applicant for a media warrant must explicitly make the issuing officer aware of the possibility that the search may involve material protected under section 68 of the Evidence Act. Failure to do so was a breach of the common law duty of candour.[42] The warrant and the ensuing search were therefore declared to be fundamentally unlawful.

8.32 The Hager case raises the wider question of whether the Search and Surveillance Act should provide greater protection for privilege, which we turn to next.

## SHOULD THE ACT PROVIDE GREATER PROTECTION FOR PRIVILEGE?

### Identifying privilege issues in applications

#### *Issues with the current law*

8.33 Currently, the Act does not require any application under it to address possible privilege claims. Yet a failure to do so risks a successful challenge to the validity of issue because candour is necessary to that process:[43]

> If nothing else, where … a [search] warrant is applied for, the judge should be satisfied not only that the police are themselves aware of these issues, but also that they have appropriate procedures in place in practice to facilitate any anticipated claim of privilege and to ensure protection of materials seized. That is to say nothing of the possibility that, properly informed, the judge could well conclude that the issue of the warrant is simply not justified in the circumstances, irrespective of the procedures provided by the Search and Surveillance Act.

8.34 This same principle of candour must apply to surveillance device warrants and examination and production orders since they are also methods of State intrusion that are authorised without notice. Privilege issues can have a role to play in the decision to issue or grant the warrant or order in all these contexts.

8.35 A production order may not just apply to routine business information held by a third party, even though this was the policy reason for their creation and is how they are currently used.[44] For example, it could be used to seek spiritual counselling records held by a minister (which might contain admissions of offending made by a person in

---

42 It also demonstrated a failure to engage with fundamentally important public interests, including the protection of free speech under the New Zealand Bill of Rights Act 1990.

43 *Hager v Attorney-General*, above n 26, at [117].

44 Search and Surveillance Act 2012, s 72. The Law Commission also acknowledged that even a suspect might be the target of such an order: Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.32]. We discuss production orders in more detail in Chapter 9.

the course of seeking spiritual guidance) or treatment records of a patient held by a clinical psychologist (which might contain similar admissions). Both situations may raise privilege issues.[45]

8.36 Examination orders require the issuing judge to be satisfied that:[46]

> … it is reasonable to subject the person to compulsory examination, having regard to the nature and seriousness of the suspected offending, the nature of the information sought, the relationship between the person to be examined and the suspect, and any alternative ways of obtaining the information.

8.37 Privilege could be relevant when considering the "nature of the information sought", the "relationship between" the examinee and suspect and whether alternative ways of obtaining the information are available. For example, answers to questions directed to an accountant about why accounts were prepared in a particular way might risk invading legal advice or preparatory materials privilege (if the instructions to the accountant were based on legal advice).

8.38 Surveillance device warrants are ongoing in their intrusion and may capture a variety of communications that could raise privilege issues, particularly in relation to intercepting legal advice.

### *Option for reform*

8.39 The Act could be amended to require an applicant for a warrant or order under the Act to identify any privilege issues of which the applicant is reasonably aware.[47]

8.40 Given that the application for a warrant or order is made ex parte, so the person whose information is sought is not able to claim their privilege at the time of the application, this additional requirement may be the only way to provide assurance that privilege will be considered by the issuing officer.

---

45 The Law Commission raised this possibility in *Search and Surveillance Powers* (NZLC R97, 2007) at [12.155].

46 Search and Surveillance Act 2012, s 38(b). We discuss examination orders in more detail in Chapter 10.

47 It is recognised that the default procedures of the Act will continue to regulate claims to privilege in the context of warrantless searches. To require Police, for example, to produce a document explaining privilege on a warrantless search (which is done under exigency) is not practicable and the absence of such a requirement in the existing legislation reflects this. In terms of the exercise of search powers where a search warrant is not required, there is again no application process in which to embed a requirement to address privilege or a document to attach such information to.

8.41 In practice, this would mean that:

- the applicant could state that there are no matters of privilege arising in relation to what is sought;
- the applicant could alert the issuing officer to a matter of privilege and assert that the procedures in the Act would be sufficient to protect the material; or
- the applicant could suggest conditions in relation to the protection of that material that the issuing officer might choose to insert.

8.42 A failure by the applicant to meet this additional requirement would operate in the same way as a failure to meet any other mandatory requirement. The issuing officer may refuse the application. If the warrant is issued or the order is granted and there is a later challenge to its execution, the failure may result in invalidity and any evidence gathered under the warrant or order risks being ruled inadmissible.

8.43 The advantage for the person whose potentially privileged material might be accessed is that this additional requirement minimises the possibility of access to such material and the subsequent use of any information derived from it.

8.44 The advantage for the issuing officer is the consistent provision of information to determine whether the warrant or order should be even issued and, if so, whether the procedures in the Act for managing privilege are adequate or whether further conditions need to be imposed.

8.45 The advantage for the applicant is a reduced risk that the search will be found to be unlawful in light of the duty of candour (which provided the basis of successful challenge to the warrant in *Hager*.)[48] Uncertainty about the extent to which privilege questions must be explored in preparing to draft the application could be mitigated by requiring "reasonable inquiry" to be made. This would be a question of judgement in the context of the particular application.

## Explaining the availability of privilege

### *Issues with the current law*

8.46 When an enforcement officer executes a search warrant they must provide the occupier of the place, vehicle or thing to be searched with a copy of the warrant before

---

[48] This situation is contemplated by *Hager v Attorney-General*, above n 26, at [117].

or on initial entry.[49] The warrant copy must contain "an explanation of the availability of relevant privileges and an outline of how any of those privileges may be claimed (where applicable)".[50]

8.47 An example of the explanation attached to search warrants has been supplied by Police and is reproduced in Appendix B. It contains a statement of the privileges that apply to search warrants, suggests accessing legal advice to explain the effect of that information and describes the duty to particularise the claim, if one is made.[51]

8.48 There is no corresponding obligation for surveillance device warrants or production and examination orders to contain any explanation.

8.49 This undermines the reason for recognising privilege in the investigation and collection phase in the first place – to promote consistency in its operation as between the investigation and the trial phases. If the privileges do not operate in the same way, material can be accessed in the investigation phase that could not be admitted at trial. Such access could allow information to be derived from that material, thereby eroding, in effect, the protective power of privilege.

8.50 Obviously in the surveillance context, the person is unaware of that surveillance and so could not claim privilege before any material is seen or heard. But it is harder to understand the variation in approach between search warrants and examination and production orders, when all privileges (including against self-incrimination) are available in relation to these orders and protection appears to depend on an actual assertion of privilege or an actual refusal to disclose the information.

8.51 We are aware that Police or other enforcement officers sometimes adopt management practices that are directed to minimising the risk of accessing material that could be the subject of a successful privilege claim. This is particularly so in relation to searches of digital material, as we discussed in Chapter 6. For example, search

---

49 Search and Surveillance Act 2012, s 131(1)(b)(i). This does not apply if it is a remote access search.

50 Section 103(4)(l).

51 In its 2007 Report, the Law Commission recommended that production orders contain a notice on the availability of privilege and how to claim it: Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [12.155]. Since the Commission did not discuss examination orders in its Report, no such recommendation was made in relation to these.

parameters might be discussed with the person's lawyer or the search of electronic records could be conducted under a lawyer's supervision.[52]

8.52 However, while enforcement officers who seek material and the professionals who hold it can be expected to know their obligations because of their training, ordinary people may not. If the availability of privilege is not written on the production or examination order, it is likely that some people subject to these orders will not know they may claim it.

8.53 The procedures in the Act for protecting privileged information may not therefore be achieving their intended object. We would like to hear from submitters about their experiences in this regard.

### *Option for reform*

8.54 The Act could be amended to require that production and examination orders explain the availability of privilege on their face.

8.55 Examination orders require answers to questions; production orders seek documents. The advantage of mandatory notification is the consistent opportunity to claim privilege before a question is answered (under an examination order) or the information or document is produced (under a production order).[53]

8.56 Parliament has already conferred privileges in relation to these orders and the requirement to notify their existence provides procedural support to enable their meaningful exercise. This will help to ensure that those rights are protected.

8.57 We can see few disadvantages in this option. Production and examination orders are made on a template form, so the explanation could be drafted once and automatically included each time. This option would therefore require no extra effort on the part of the applicant.

Q35 Is privileged material adequately protected during the exercise of search or surveillance powers by the existing procedures? If not, what are the impediments to protecting privileged material?

Q36 Is it clear when and how privilege claims can be made?

---

[52] It is assumed this same practice could also apply if the search were conducted in another professional context, such as a search of electronic material held by a medical practitioner or clinical psychologist or by a minister.

[53] It has been noted that the drafting of the grounds for a production order has a wider forensic reach than their current use might suggest. For example, they could be directed to a suspect.

Q37 Should the Act be amended to provide greater protection for privileged material? For example, by:

(a) requiring the enforcement officer applying for a warrant or order to identify potential issues of privilege; and/or

(b) requiring production orders and examination orders to explain the availability of privilege and how to claim it?

## THE PRIVILEGE AGAINST SELF-INCRIMINATION

### Should the privilege apply to production orders?

#### *Issues with the current law*

8.58 As noted above, the Act provides that the privilege against self-incrimination (as described in section 60 of the Evidence Act) can be claimed in relation to production orders and examination orders.[54] However, it appears that in practice the circumstances in which the privilege can apply in the context of production orders is very limited, or perhaps non-existent. A question therefore arises as to whether the privilege should continue to be available in respect of production orders.

8.59 Prior to the Evidence Act, the common law made a distinction between pre-existing documents and testimonial evidence. Testimonial evidence is a statement made in response to a question (in contrast to evidence admitted as an object). The common law generally applied the privilege against self-incrimination only to testimonial evidence. This is because the privilege only provides protection against a person incriminating him or herself. It does not protect against anything that is incriminating.

8.60 The Law Commission's review of evidence law, published in 1999 (and referring to its earlier Discussion Paper on self-incrimination), recommended that the privilege should not apply to pre-existing documents because the underlying interests said to be served by the privilege were not served in respect of that type of evidence.[55] Specifically:[56]

- the likelihood of compulsion causing the evidence to be unreliable or created from an abuse of power is minimal;

---

54 Search and Surveillance Act 2012, s 138.

55 Law Commission *Evidence: Reform of the Law* (NZLC R55, 1999) at [280]–[281]; Law Commission *The Privilege Against Self-Incrimination* (NZLC PP25, 1996).

56 Law Commission *The Privilege Against Self-Incrimination* (NZLC PP25, 1996) at [203].

- there is no risk that an innocent person will speak rashly or ill-advisedly because the document is already in existence;
- pre-existing evidence is less likely to be unreliable than other forms of evidence, such as confessions;
- while privacy concerns may be relevant in relation to pre-existing documents, they should not prevail over the concern to obtain all relevant evidence; and
- any concern to maintain a fair balance between the State and the individual can be adequately addressed by the prohibition on unreasonable search and seizure in section 21 of the New Zealand Bill of Rights Act 1990.

8.61 These recommendations were reflected in section 60 of the Evidence Act, which limited the application of the privilege to statements given either orally or in a document that is prepared or created in response to a requirement to provide specific information. "Information" is defined as:[57]

> … a statement of fact or opinion given, or to be given,—
>
> (a) orally; or
>
> (b) in a document that is prepared or created—
>
> (i) after and in response to a requirement to which any of those sections applies; but
>
> (ii) not for the principal purpose of avoiding criminal prosecution under New Zealand law.

8.62 That information must be reasonably likely to lead to, or increase the likelihood of, the prosecution of a person for a criminal offence.[58]

8.63 As we describe in the following chapter, production orders require the disclosure of documents either on one occasion only or on an ongoing basis.[59] However, while a production order can relate to documents not yet in existence, those documents are not prepared or created in response to a requirement to provide specific information. Rather, they will generally have been prepared for the normal business purposes of the third party required to produce them.

---

57 Evidence Act 2006, s 51(3).

58 Section 4 (definition of "incriminate").

59 Search and Surveillance Act 2012, s 71(2)(g).

8.64 It therefore appears that, in practice, there is no scope for the privilege against self-incrimination to operate in respect of production orders.[60]

### *Option for reform*

8.65 If that assessment is correct, the issue for this review is whether section 138 of the Act (which states how the privilege against self-incrimination applies under the Act) should be amended to remove the meaningless reference to production orders. The advantage of such a reform is that it would bring clarity to the issue. If there is no scope for the privilege to operate, court and enforcement agency resources will be occupied for no good reason where such a claim is made and inevitably ruled to be unsuccessful. Also, there would appear to be no negative impact on the status quo if it is correct that the provision currently has no application.

## How should the privilege apply to requests for access information?

### *Issues with the current law*

8.66 The privilege against self-incrimination is also mentioned in section 130 of the Act. Section 130 empowers a person executing a search power in respect of a computer system or other data storage device to require a specified person to provide access information and other information or assistance that is reasonable and necessary to allow access to the data.

8.67 Section 130 is useful for law enforcement investigations. It is commonly used to require the passcodes or encryption keys for mobile phones and other electronic devices. Enforcement agencies expect to increasingly rely on it as encryption becomes the default setting on many electronic devices. While some law enforcement investigators have access to tools to unlock devices, those tools may not always be available or effective, or they may take too much time.

8.68 However, subsections (2) and (3) of section 130 create some difficulty. They provide:

> (2) A specified person may not be required under subsection (1) to give any information tending to incriminate the person.
>
> (3) Subsection (2) does not prevent a person exercising a search power from requiring a specified person to provide information or providing assistance that is reasonable and necessary to allow the person exercising the search power to access data held in, or accessible from, a computer system

[60] We note that the authors of *Adams on Criminal Law – Rights and Powers* reach the same conclusion. See Simon France (ed) *Adams on Criminal Law – Rights and Powers* (online looseleaf ed, Thomson Reuters) at [SS136.16].

or other data storage device that contains or may contain information tending to incriminate the specified person.

8.69 Subsection 2 states, on the one hand, that a person providing assistance under the section may not be required to incriminate him or herself. On the other hand, the effect of subsection 3 appears to be that this protection does not extend to the provision of information or assistance to allow access to data held in the computer system or data storage device.

8.70 We have encountered two types of concerns about subsection 130(3). The first concern is simply that the provision is too difficult to understand. The subsection replaced section 198B of the Summary Proceedings Act 1957, which served the same policy purpose, but was easier to understand. We consider that, at the very least, the provision would benefit from redrafting to make it more accessible.

8.71 The second concern is that subsection 130(3) appears to leave very little space for the privilege outlined in subsection 130(2) to operate.[61] This was raised in 2010 in three submissions to the Select Committee when the Search and Surveillance Bill was going through the House. One submitter argued that requiring a person to do something that will enable access to information that incriminates them is the same as requiring that person to incriminate themselves. In response, the departmental report provided to the Select Committee said that access information, in and of itself, does not constitute self-incriminating material because it does not amount to evidence of an offence. The provisions therefore did not impinge on the privilege against self-incrimination.[62]

8.72 We consider that an understanding of the privilege as it applies in the Evidence Act helps to clarify the rationale behind these subsections. As we described above, the privilege in that Act does not apply to pre-existing documents because it is only designed to protect against incrimination that a person might do to him or herself. In relation to a search of a computer system or data storage device to which access assistance might be requested under section 130, the documents on that system or device are pre-existing, and so are not protected by the privilege. In theory, the statement in which the access information or encryption key is provided would be testimonial evidence because it is a statement made in response to a question.

---

61 See for example Tania Singh and Nick Chisnall "Warrantless searches of electronic devices" [2014] NZLJ 419–421.

62 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [444].

However, that information is generally not evidence (or incriminating) in its own right. Its only purpose is to provide access to something that is not otherwise protected by the privilege.

8.73 That said, there could be some circumstances in which the access information amounts to evidence in its own right. For example, if ownership or control of the computer system or data storage device is a live issue in the investigation, the fact that a person knows the access information or encryption key could provide evidence of that ownership or control. Currently, section 130(3) does not allow the privilege to be claimed in relation to access information that, by itself, tends to incriminate.

8.74 We note that section 198B of the Summary Proceedings Act did allow for a claim of privilege in relation to access information that would, by itself, tend to incriminate the person. Subsections (3) and (4) provided:[63]

> (3) A person may not be required under subsection (1) to give any information tending to incriminate the person.
>
> (4) Subsection (3) does not prevent a constable from requiring a person to provide information that—
>
> (a) is reasonable and necessary to allow the constable to access data held in, or accessible from, a computer that—
>
> (i) is on premises named in the warrant concerned; and
>
> (ii) contains or may contain information tending to incriminate the person; but
>
> (b) *does not itself tend to incriminate the person.*

### *Option for reform*

8.75 As we noted above, subsection 130(3) replaced section 198B(4) of the Summary Proceedings Act, but it is harder to understand. It also omits the paragraph (paragraph 4(b) in the Summary Proceedings Act provision) that would extend the protection of the privilege against self-incrimination to the provision of access information if that information by itself tends to incriminate the person providing it. An option to address these issues is to amend the provision to make it easier to understand and to include that omitted paragraph. This would resolve much of the current confusion and provide better protection for the privilege against self-incrimination (consistently with the Evidence Act).

---

[63] Emphasis added.

Q38 Is there any scope for the privilege against self-incrimination (as described in section 60 of the Evidence Act) to apply to production orders? If not, should this be clarified in the Act?

Q39 Does section 130(3) adequately explain when the privilege against self-incrimination can be claimed?

Q40 Should section 130(3) be amended so that a person can decline to provide access information that is, itself, incriminating, in reliance on the privilege against self-incrimination?

# Chapter 9 – Production orders

## BACKGROUND

9.1 Prior to the Search and Surveillance Act 2012 (the Act), enforcement officers who wanted to obtain data from a third party, such as a telecommunications company or a bank, would obtain a standard search warrant.[1] While search warrants are normally executed by the applicant actually searching the premises for the evidence him or herself, the common law provided that where the thing to be seized was held by a cooperative third party, the warrant could be executed by merely sending the warrant to the organisation named.[2]

9.2 In its 2007 Report, *Search and Surveillance Powers*, the Law Commission recommended introducing a specific form of authorisation for these types of searches – to be called production orders. The main rationale for these orders was that it is easier for the person against whom the order is made to locate the information than it is for the enforcement officer.[3] It will generally be less disruptive to a third party business to comply with a production order than with a standard search warrant and it will usually reduce the amount of irrelevant material seen by the enforcement officer.[4]

9.3 The Commission noted a number of potential disadvantages of introducing production orders – namely, that it may add complexity to the search regime and be confusing to have two processes for the same information.[5] However, ultimately it thought that a production order would better reflect the nature of the transaction and would provide a less intrusive form of search power.

---

1 In this chapter, we use the term "third party" to refer to the entity against which a production order is made. While production orders are usually made to obtain information about a person who is a customer of an organisation against which the order is made, it is possible for them to be made against any person or entity, including against a person who is a suspect or later becomes a suspect.

2 *R v Sanders* [1994] 3 NZLR 450 (CA).

3 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.18].

4 In its final report on the Search and Surveillance Bill, the Select Committee noted that there had been some misunderstanding about the nature of the production order regime and that they were intended to provide a less intrusive alternative to a search warrant in circumstances where the party subject to the order was willing to cooperate with enforcement officers: Search and Surveillance Bill 2010 (42-2) (select committee report) at 11.

5 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.20].

9.4 The Commission also considered whether there should be a lower threshold for issuing production orders for specific types of information, such as account holder information from financial institutions. However, it did not recommend a lower threshold because it thought there was nothing to distinguish that type of information from other types of information and a lower threshold would be seen as sanctioning fishing expeditions.[6]

## Current law

9.5 The Act generally reflects those recommendations. It states that any enforcement officer who has a power to apply for a search warrant in respect of documents may apply for a production order for those documents.[7] He or she must have reasonable grounds to:[8]

- suspect that an offence has been, is being or will be committed (being an offence for which that officer may apply for a search warrant); and
- believe that the documents constitute evidential material in respect of the offence and are in the possession or under the control of the person against whom the order is sought (or will come into their possession or under their control while the order is in force).

9.6 This threshold for the issuing of production orders is equivalent to the threshold for search warrants. Also, as with search warrants, the section *empowers* the enforcement officer to get a production order, rather than specifying when he or she *must* get one. However, unlike a search warrant, which provides a power for the enforcement officer to search for the targeted material him or herself, a production order requires the third party to provide the information. If the third party fails to comply with the order without reasonable excuse, that person or entity is liable on conviction to a term of imprisonment not exceeding one year (for an individual) or a fine not exceeding $10,000 (for a body corporate).[9]

9.7 It should also be noted that a production order under the Act may be made against *any* person. That could be an individual or a legal entity, or even a suspect. It is not limited

---

6 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.26].

7 Search and Surveillance Act 2012, s 71.

8 Section 72.

9 Section 174.

to commercial companies and there is no condition that the person or company is considered to be cooperative.

9.8 Many of the provisions relating to search warrants also apply to production orders. In particular:

- the issuing officer may require the applicant to supply further information;[10] and
- applications must generally be in writing but the issuing officer may allow an oral application to be made (for example, by telephone) if the required information is supplied, the issuing officer is satisfied that the delay caused by a written application would compromise the effectiveness of the search, and the matter can be properly determined orally.[11]

## How production orders are used

9.9 Production orders are one of three mechanisms by which enforcement agencies can obtain information from a third party. The other two mechanisms are by voluntary disclosure and by other statutory powers. Under the voluntary disclosure mechanism, an agency simply requests the information from the third party without relying on any legal authority, just as it can ask questions of any person who may have relevant information about offending.[12] It is up to the third party to decide whether it will voluntarily release the information. Where the information sought is personal information, an information privacy principle under the Privacy Act 1993 permits its release to an enforcement officer if:[13]

> … it is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.

9.10 It is important to be clear that this principle does not empower the enforcement agency to ask for the information. It merely permits the third party to release it. We also note that a third party company that receives regular requests for customer information from enforcement agencies may have an agreed protocol or Memorandum of Understanding with the agency covering what type of information the company will voluntarily release and what it will require a court order for.

---

10 Search and Surveillance Act 2012, s 73(2)(a).

11 Section 73(2)(c).

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

13 Privacy Act 1993, s 6, principle 11(e).

9.11 There are a number of statutory provisions that empower agencies to request information from third parties for law enforcement purposes. Some of those powers require a court order,[14] but many are exercised on the authority of a person acting under the relevant Act. This latter category includes:[15]

- section 17 of the Tax Administration Act 1994, which enables the Commissioner of Inland Revenue to require any person to provide information or produce documents for inspection which the Commissioner considers necessary or relevant for the administration or enforcement of any of the Inland Revenue Acts or any other function of the Commissioner;[16] and
- section 11 of the Social Security Act 1964, which enables the Chief Executive of the Ministry of Social Development to require any person to provide information, produce documents or furnish copies or extracts of a document or record for a range of purposes under that Act, including determining whether a person claiming a benefit is entitled to receive that benefit.[17]

9.12 Production orders are used by many government agencies with law enforcement functions, including New Zealand Police, the Department of Internal Affairs and the Ministry for Primary Industries. Examples of how they are used include:

- in a child pornography investigation, to obtain the IP address of a suspect;
- in an animal welfare investigation, to obtain the animal's health records from the suspect's veterinarian;
- in a fisheries investigation, to obtain the bank records of a person suspected of illegally selling fish.

Any enforcement officer who can apply for a search warrant can also apply for a production order.

---

14 For example, s 42 of the Fair Trading Act 1986 enables the Commerce Commission to apply to a court for an order requiring a person to disclose information if the court is satisfied the person has engaged in conduct contravening Parts 1 to 4 of that Act.

15 Privacy Commissioner *Transparency Reporting Trial Aug–Oct 2015: Full Report* (2016). Appendix B lists 51 information gathering powers under a variety of statutes, but not all of these relate to law enforcement purposes.

16 See *New Zealand Stock Exchange v Commissioner of Inland Revenue* [1990] 3 NZLR 333 (CA).

17 See *Reed v R* [2014] NZCA 525 at [32]–[37].

9.13 Agencies do not routinely publish statistics on the number of requests they make for information from third parties – whether by production order or other mechanisms.[18] However, a recent trial of transparency reporting by the Privacy Commissioner provides an indication. This trial follows an emerging international trend for large telecommunications and internet companies to publish transparency reports. Those reports provide statistics on the number and nature of requests received by a company from government agencies for personal information about their customers.[19]

9.14 The Privacy Commissioner's trial, which ran across a three-month period (August to October) in 2015, was designed to better understand how it could assist companies in this type of reporting. Ten companies agreed to produce standardised transparency reporting information. They included two telecommunications companies, seven financial services companies, and one utility company.[20]

9.15 In summary, the Privacy Commissioner reported that over the three-month trial period:[21]

- the participants received 11,799 requests for customers' information;
- 11,349 of those requests were accepted in full, one was partially accepted and 449 were declined; and
- the bulk of requests came from Inland Revenue (4,670 requests), Police (3,513 requests), and the Ministry of Social Development (3,150 requests).

9.16 The trial found that 962 requests were made under a production order (that is, approximately 8 per cent of the total requests) and roughly twice as many were by voluntary disclosure. The majority were made under statutory powers of authority, particularly section 17 of the Tax Administration Act or section 11 of the Social Security Act.[22]

---

18 Below at paragraph [9.60] we ask whether enforcement agencies should be required to report annually on the number of production orders for which they apply.

19 Wikipedia, The Free Encyclopedia "Transparency Report" <https://en.wikipedia.org/wiki/Transparency_report>. We also note that in New Zealand, Trade Me began publishing an annual transparency report in 2013, detailing requests for information from Police, other government departments and the Disputes Tribunal. Trade Me's transparency reports can be found at <www.trademe.co.nz/trust-safety/2016/7/22/trade-me-transparency-report-2016/>. We are not aware of any other New Zealand companies that are currently publishing this type of data.

20 Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 11.

21 At 13.

22 At 28.

9.17 This trial gives us an indication of how production orders fit into the range of mechanisms available to government agencies for obtaining information from third parties.[23] It is not a reliable indicator of the number of production orders made (because the ten companies involved in the trial represent only a subset of all the companies from which information may be sought under a production order). It should also be noted that requests for information under the other mechanisms will, in some cases, be for non-law enforcement purposes (for example, finding missing persons).

9.18 We have been told by enforcement agencies that, in practice, the choice of mechanism that is used to obtain information will depend upon a number of factors, including:

- the stage of the investigation;
- the nature of the information sought and whether the officer considers that a request for it may invade reasonable expectations of privacy; and
- prior knowledge of the requirements of the third party from whom it is sought.

9.19 In many cases, voluntary disclosure of information is sought when the investigation is still at an early stage and the thresholds for a production order cannot be met. That is, there may not yet be reasonable grounds to suspect that an offence has been, is being, or will be committed, nor reasonable grounds to believe that the documents sought are in the possession or control of the person against whom the production order would be made. In the earlier stages of an investigation, Police will sometimes not know what information is held or by whom it is held.

9.20 In other cases, officers make an assessment as to whether the information sought may later be held to have been improperly obtained and perhaps be ruled inadmissible as evidence in criminal proceedings under section 30 of the Evidence Act 2006. If that is a concern, there is an incentive to apply for a production order. In effect, officers assess whether the information request may be considered to invade reasonable expectations of privacy. Generally, the more invasive the information sought, the more likely that either the third party will require a production order or the enforcement officer will seek to protect the future admissibility of the information by applying for a production order.

---

[23] In addition, Trade Me's 2015 transparency report states that in that year, the greatest number of inquiries for personal information came from Police (1,840 inquiries), the Ministry of Business, Innovation and Employment (175 inquiries), the Ministry of Social Development (95 inquiries) and the Commerce Commission (91 inquiries).

9.21 A number of issues arise from these legal and practical aspects of production orders:

- whether the Act should be clearer about when a production order is required;
- whether enforcement agencies should be required to report on the number of production orders they apply for; and
- whether people should be notified when their information is sought from a third party by a production order.

9.22 We discuss each issue in turn.

## SHOULD THE ACT BE CLEARER ABOUT WHEN A PRODUCTION ORDER IS REQUIRED?

9.23 We have encountered some concern (noted in the Privacy Commissioner's report on its transparency trial)[24] that enforcement officers are sometimes obtaining information by voluntary disclosure when it is thought they should be applying for a production order.[25] They are able to choose to request the voluntary disclosure of information because the Act does not specify when a production order must be obtained. The question for this review is whether the Act should be clearer as to when a production order is required.[26]

9.24 The types of information sometimes obtained by enforcement officers by voluntary disclosure include:

- electricity consumption data from an electricity supplier;
- airline travel information, including immediate and future travel plans;
- identification details from a company's customer database, linked to a telephone number or email address supplied by the enforcement agency; and
- metadata associated with the use of a phone (for example, indicating which cell phone sites the phone has linked to and when that occurred).

9.25 This issue is really a subset of the broader issue discussed in Chapter 2 as to whether the Act should be more specific about when a prior authorisation for any type of

---

24 Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 6.

25 See also David Fisher "Police Given Personal Information Without Search Warrants" *The New Zealand Herald* (online ed, Auckland, 25 March 2015); and Nick Grant "Hager Adds New Claim in Action Against Police" *The National Business Review* (online ed, Auckland, 5 April 2016).

26 We note that the Supreme Court is currently considering a case that raises issues about the use of requests for voluntary disclosure instead of production orders. The case is subject to suppression orders until final disposition of the trial.

search is required.[27] As was explained in that chapter, the Act also does not specify when a search warrant is required.

9.26 This issue arose in the context of a police investigation into the identity of the person known as "Rawshark", who supplied information to journalist Nicky Hager for his book *Dirty Politics*. As we described in Chapter 8, Police were investigating the identity of "Rawshark" and whether he or she had committed an offence by unlawfully accessing the computer of blogger Cameron Slater. In pursuing this investigation, Police sought information about Mr Hager from a number of banks, telecommunications companies and airlines without first obtaining a warrant or production order. Most refused the request but one bank complied and provided details of Mr Hager's accounts.[28] There was considerable public interest in this story with several commentators questioning whether Police should be able to request this type of information without a warrant or production order, and whether a bank should be able to supply it.[29]

## Possible concerns with the current approach of the Act

9.27 The current approach in the Act of empowering enforcement officers to apply for production orders rather than describing when they must be obtained could be seen as having a number of disadvantages.

### *Lack of clarity and consistency about when the Act should be applied*

9.28 By not specifying when a production order is required, the Act leaves that decision to enforcement officers and the people who hold the information (usually a third party). In the absence of specific guidance in the Act, there appears to be a broad spectrum of opinion as to when a production order is required. Some consider that by enacting a production order regime in the Act, Parliament must have intended that it be used for every request. Others consider that the words of the statute cannot be interpreted as

---

27 See paragraph [2.89] above.

28 David Fisher "Police Got Hager Data Without Court Order" *The New Zealand Herald* (online ed, Auckland, 24 October 2015).

29 Rick Shera "Privacy Implications of Westpac's Release of Nicky Hager's Personal Information" *The National Business Review* (online ed, Auckland, 31 October 2015); Shannon Gillies "Westpac Under Fire for Hager decision" *Radio New Zealand* (online ed, Wellington, 28 October 2015); and Anthony Robins "Angry at Westpac" (26 October 2015) The Standard <https://thestandard.org.nz/angry-at-westpac/>.

overriding the enforcement officer's freedom to ask for any information by voluntary disclosure.

9.29 Described in another light, this is a question as to whether the principle in *R v Thompson* remains good law since the enactment of the Act.[30] In that case, Police obtained electricity consumption information from an electricity supplier without a warrant. The Court of Appeal said that it was not unlawful for the police officer to make the inquiry without a warrant and for the electricity supplier to supply the information. It held that the disclosure "came squarely within exception (e) of Principle 11 of the Privacy Act 1993".[31] We consider that, in the absence of clear guidance from the Act as to when a production order must be obtained, it is not clear whether *Thompson* remains good law and, accordingly, when a production order must be obtained.

### *Officers applying reasonable expectations of privacy test*

9.30 It may be thought that enforcement officers are not well-placed to determine whether a production order should be applied for in individual circumstances. As described above, one of the key considerations when they make that decision is whether obtaining the information would invade reasonable expectations of privacy. However, as we described in Chapter 2, determining whether a search (or in the case of a production order, a request for information) might invade reasonable expectations of privacy will often involve a highly nuanced assessment. It may be unrealistic to always expect enforcement officers to make that assessment accurately.

### *Retrospective recognition of rights*

9.31 Another concern might be that by leaving the determination as to whether a production order is required to the enforcement officer, the Act provides little proactive protection of privacy rights. If the enforcement officer gets it wrong, the main way for a person to challenge the decision of the enforcement officer is to challenge the admissibility of

---

30 *R v Thompson* (2000) 18 CRNZ 401, [2001] 1 NZLR 129 (CA).

31 At [54]. Principle 11(e) of the Privacy Act 1993 provides (amongst other things) that an agency holding personal information may disclose that information to a person, body or agency where the agency believes on reasonable grounds that this is necessary "to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences". This aspect of the decision was not discussed in Law Commission *Search and Surveillance Powers* (NZLC R97, 2007).

the information if it is introduced as evidence in proceedings. That may amount to a fairly weak protection of rights because it occurs a considerable time after the information is supplied and such a challenge can only be mounted in relation to information that becomes evidential material.

9.32 In contrast, if the Act describes when a production order is required, the request for information covered by that provision would be subject to an issuing officer's consideration as to whether the threshold for making a production order is met.

9.33 In theory, it may also be possible to judicially review a decision to obtain information by voluntary disclosure rather than by production order. However, this would only provide retrospective recognition of rights and, in any event, the courts have been concerned about the use of judicial review proceedings to challenge search warrants prior to criminal charges being laid. Similar concerns may apply to any challenge to a decision to seek information without a production order.

9.34 In the leading case, *Gill v Attorney-General*, Dr Gill challenged a warrant authorising a search of her medical practice by way of judicial review.[32] The challenge occurred when the investigation was still proceeding and before any criminal charges had been laid. It had the effect of temporarily halting the investigation. The Court said that the issues arising under that challenge—relevance and the admissibility of evidence—would be more appropriately dealt with as direct challenges to the admissibility of evidence once charges were laid. It indicated that judicial review should be reserved for cases where:[33]

> … the defect in the search warrant is of a fundamental nature, where the matter could be said to go to the jurisdiction of the issuing officer or where some other ground of true unlawfulness (such as want of jurisdiction) is established.

9.35 This principle was recently applied in *Hager v Attorney-General* where the High Court observed that an application for judicial review should not be entertained unless it is a clear case of an unlawful search and seizure of a fundamental kind.[34] It therefore appears that in the absence of statutory rules about when a production order must be obtained, it would be a very rare case where a request for the voluntary disclosure of information could be challenged by judicial review.

---

32 *Gill v Attorney-General* [2010] NZCA 468, [2011] 1 NZLR 433.

33 At [20].

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

### *Third parties as decision-makers*

9.36 As we described above, it can be the third party against whom a request for information is made that determines whether or not a production order is required. In our view, arguably these third parties are also not well-placed to be making that decision.

9.37 When a third party is making that decision, it will often be applying the exception in the Privacy Act 1993 to the usual rule of non-disclosure of personal information – that disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency.[35] Some possible concerns with this type of decision include:

- the threshold is too low (it is obviously lower than the threshold for making a production order);
- decisions about disclosure of information should be made by a publicly accountable decision-maker rather than the holder of the information, on the basis that the holder has motivations that may conflict with the protection of the privacy interests of its customers; and
- these third parties might not have sufficient information to determine whether disclosure is necessary in the circumstances.

9.38 On this final point, we have heard anecdotally (from people we have had preliminary discussions with) that sometimes very limited details of the investigation are provided when requests for personal information are made without a production order or warrant. At the very least, it is likely that there are a variety of practices across the thousands of requests for information without a production order or warrant for law enforcement purposes that are made every year. Also, there is likely to be a range of views as to the type of assessment that should be conducted before being satisfied that disclosure is necessary.

9.39 Interestingly, one commentator on the *Hager* case pointed out that police requests for information from third party organisations look very official – they contain the police crest, are set out like a legal document and contain formal language. The implied

---

[35] Privacy Act 1993, s 6, principle 11(e). See footnote 31 above.

concern is that it may not be clear to a less sophisticated third party that they have an option to decline the request.[36]

## Advantages of the current approach

9.40 Despite the concerns outlined above, there are also a number of advantages to the current approach, which gives enforcement officers the option to seek information from third parties either on a voluntary basis or via a production order.

### *Avoiding cost and delay*

9.41 The biggest advantage to enforcement officers is that the approach enables greater efficiency in investigations. If the Act requires more requests for information to be made only with a production order, that would have a significant impact on costs and delay in investigations.

9.42 Police and other enforcement agencies rely heavily on the voluntary provision of information for much of their work. Together, they make tens of thousands of requests for information on a voluntary basis from third party organisations every year. For example, Police told us that:

- in a recent 12-month period there were 29,750 requests for information to telecommunication companies in relation to 111 emergencies,[37] attempted suicides, firearms incidents, kidnappings and child abductions, bomb threats and threats to kill;
- on 25 April 2016 there were 3,499 "agreed Child Protection Protocol" cases, meaning that Police and Child, Youth and Family were jointly investigating allegations of serious child abuse and voluntarily sharing information under the Privacy Act.[38]

9.43 Police tell us that an application for a production order can take four to six hours to prepare and obtain from an issuing officer. It could be shorter if the enforcement officer has easy access to a court house, but longer (sometimes several days) for more complex applications. Applications are usually in writing. There is provision for them

---

[36] Rick Shera "Privacy Implications", above n 29.

[37] See for example *Arnerich v R* [2012] NZCA 291 at [18].

[38] Police also have Approved Information Sharing Agreements with the Inland Revenue Department and the Ministry of Social Development under which personal information is voluntarily shared in reliance on the exceptions in the Privacy Act 1993.

to be made by telephone call or by personal appearance, but first the issuing officer must be satisfied that:[39]

- the delay caused by requiring a written application would compromise the effectiveness of the search;
- the question of whether the production order should be issued can properly be determined on the basis of an oral communication or a personal appearance; and
- all the necessary application information in section 98(1)–(3) is supplied.

9.44 Even an oral application for a production order would require significantly more time to gather the requisite information than an informal request based on voluntary disclosure.

### *Enabling provision of evidence*

9.45 We are told that many requests for the voluntary disclosure of information are made at a point in the investigation at which enforcement officers do not have sufficient evidence to support an application for a production order. There is a concern that statutory amendments to require production orders for those types of requests would prevent some investigations from proceeding. Frequently, information obtained from third parties by voluntary disclosure provides the evidence to meet the threshold requirements for obtaining a subsequent search warrant or production order. For example, an enforcement officer might ask an organisation to voluntarily disclose whether a person is a customer so that they can then obtain a production order against that organisation for the customer's information. If more requests for information require a production order, it is feared that investigations will not be able to proceed because the thresholds could not yet be met.

9.46 Similarly, in many instances a person or entity providing information voluntarily is a witness to the offending or is able to supply a record of it occurring. Examples include a bystander who sees an assault occur or a service station that supplies video footage of a robbery occurring on its premises. It cannot be envisaged that a production order would be required before that type of information is supplied. It is and has always been part of the core role of Police to speak to witnesses and victims of crime to piece together information about what has occurred.

---

[39] Search and Surveillance Act 2012, s 100(3).

### *Enabling more refined requests*

9.47 We have encountered an argument that requests for information on a voluntary basis may be less intrusive of privacy than requests based on compulsion under a production order or other statutory power. If the request is received informally, the organisation can evaluate the precise nature of the information required for the investigation and only supply that. A production order will include a description of the information required to be produced, which will often be somewhat broader in scope than the precise information required.

9.48 Trade Me made this point in its 2016 Transparency Report:[40]

> In many ways, it's better for our members when we work under the Privacy Act as it gives us the ability to better control the amount and relevance of information released. This ensures irrelevant member data isn't caught up in the release and the requester only gets what's really useful. Put another way, this approach allows us to use a scalpel rather than a chainsaw.
>
> Compulsion orders, on the other hand, can be wide in scope and will often require the release of information that may not be directly relevant to the matter under investigation. We're legally required to comply with compulsion orders, regardless of scope.

9.49 The report gave the following example:[41]

> … if [the Ministry of Business, Innovation and Employment] was investigating a car seller to determine if they should be registered under the Motor Vehicle Sales Act, a Privacy Act release would allow us to only release sales data that covered motor vehicle sales, not the seller's full sales history which could be legally required under a compulsion order.

9.50 This is an interesting point. However, we consider it can only be argued that voluntary disclosure is a better method than compulsion for minimising the risk of disclosing irrelevant data when the organisation holding the information has a strong interest in protecting the privacy of its customers. Where that is not the case, it could be argued that compulsion (and therefore, consideration of the threshold by an issuing officer) is a better method. Also, Trade Me's concern could also be addressed if production orders were more specific in the description of the information sought.

## Options for reform

9.51 If it was thought that the Act should be clearer about when a production order is required, the Act would need to define what types of information requests that rule

---

[40] Trade Me *Transparency Report* (2016) at 4, available at <www.trademe.co.nz/trust-safety/2016/7/22/trade-me-transparency-report-2016>.

[41] As above.

applies to. It is not contemplated that Police should never obtain information by voluntary disclosure, or else Police could not talk to potential witnesses.

### *Reasonable expectations of privacy*

9.52 In Chapter 2 we discussed whether the Act should introduce a mandatory residual warrant regime or require authorisation for all search and surveillance activities and, if so, how the Act should define the conduct covered by such provisions.[42] We offered two options for defining what conduct should require prior authorisation (whether by a warrant, statutory power or other form of authorisation):[43]

- conduct that invades a reasonable expectation of privacy; or
- an alternative two-part test focusing on the type of information sought and whether it is publicly available.

9.53 If the Act were amended to require authorisation for all search or surveillance activities falling within either of those definitions—or any other definition developed—that test could also apply to information sought from third parties. In that case, it may not be necessary to have a separate test that sets out when production orders are required. If it was not considered appropriate to require a production order for all requests for information falling within the definition, the Act could specifically permit voluntary disclosure in certain circumstances.

9.54 Alternatively, whether or not that type of amendment was made, the Act could be amended to include a specific test for when a production order must be obtained. We have developed two further possible options.

### *Type of entity from which it is requested*

9.55 The Act could state that a production order is required for certain types of information from certain types of entities. Those descriptions could be either general or specific. For example:

- any documents held by any person or entity that holds the information sought in the normal course of business; or
- any documents held by the following types of goods or service providers:

---

42 See paragraphs [2.89] and [2.105] above.

43 See paragraphs [2.107] and [2.112] above.

- telecommunications service providers;
- internet service providers;
- financial services providers;
- electricity and gas suppliers; or
- transport services providers.

9.56 The disadvantage of this option is that it is somewhat arbitrary. It does not capture with precision all requests for information that may invade a reasonable expectation of privacy. It is likely to capture either too many requests (and therefore have an unjustifiably chilling effect on law enforcement investigations) or too few requests (and therefore provide insufficient protection of privacy interests).

### *Production orders as the default position*

9.57 Another option is for the Act to state that enforcement officers must obtain a production order, if it is possible to do so without prejudicing the investigation. In effect, this would make production orders the default position and enforcement officers would have to show that they had good reasons related to the investigation for not obtaining a production order.

9.58 However, this option may be of limited utility. It is likely that the majority of requests for voluntary disclosure of information would be made:

- under time pressure because the information sought (or evidential material that might flow from that information) might be lost or deleted; or
- where the thresholds for a production order could not yet be reached.

9.59 In both these cases, obtaining a production order would not be possible and so a request for voluntary disclosure of information could be made. It is likely that the only cases captured by this test would be those where there is no time pressure or the investigation has advanced to the point where the threshold for a production order is met.

Q41 Should the Act specify when a production order must be obtained?

## REPORTING REQUIREMENTS

9.60 It has been suggested to us (from people we have had preliminary discussions with) that the Act should require enforcement agencies that use production orders to report

annually on the number they have applied for, as they are required to do in relation to other orders.

9.61 Currently, the Commissioner of Police and the Chief Executive of any enforcement agency exercising search or surveillance powers under the Act are required to report annually on their use of warrantless powers for entry, search or surveillance; surveillance device warrants; and declaratory orders. They must report the numbers granted or refused in the relevant year and provide certain details about the nature of the orders made.[44] Police are also required to provide similar information about examination orders.[45]

9.62 These requirements followed similar recommendations in the Law Commission's 2007 Report.[46] The Commission said that this type of reporting serves two purposes:[47]

> … it provides a layer of accountability by providing information to Parliament on the exercise of coercive powers specifically authorised by the legislature; and it requires information regarding the exercise of such powers to be collated in a publicly available document.

9.63 The Commission recognised that the advantages of transparency and having the powers collated for research purposes must be balanced against the administrative burden that such reporting requirements impose.[48] It thought that annual reporting was justified for warrantless searches because they are not subject to the same external scrutiny as powers exercised under warrant; and for surveillance device warrants because they are almost always exercised covertly, which increases the need for accountability and transparency.[49]

9.64 In relation to production orders, one of the main reasons for annual reporting would be to assess whether the power is being used appropriately. Some questions in relation to production orders that may be of public interest might include:

---

44 Search and Surveillance Act 2012, s 172.

45 Section 170(1)(c).

46 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [4.45]. We note that the Commission's recommendation was in relation to "residual warrants", which were changed to "declaratory orders" during the legislative process. Similarly, examination orders were not discussed in the Commission's Report.

47 At [15.45].

48 At [15.46].

49 At [15.47]–[15.48]. The Commission did not discuss whether there should be a reporting requirement in relation to production orders in its Report.

- Are the numbers of production orders that are applied for increasing or decreasing over time and if so, why is that?
- To what extent and in relation to what type of information and what type of organisations are enforcement agencies obtaining information by voluntary disclosure rather than by production orders?
- Are there regional differences in the number or nature of production orders?
- Are production orders placing an unreasonable burden on some entities?[50]

9.65 Annual reporting of simply the number of production orders applied for would only be relevant to the question of the increase or decrease in numbers over time. It would not provide information as to the cause of that trend. Other information that might elucidate that trend or answer the other questions would include:

- the nature of the offences in relation to which production orders were applied for;
- the type of information sought under production orders;
- the number of requests for voluntary disclosure of information (and the type of information sought); and
- a regional breakdown of the information above.

9.66 The issue for this review is whether there is sufficient benefit to be gained from requiring enforcement agencies to report on production orders to justify the cost to those agencies in gathering the statistics. It is possible that the benefit will only be gained if the requirement covers some other details beyond the bare number of production orders applied for each year. If so, that increase in benefit must again be weighed against the increase in compliance costs. We note that, given the high number of production orders applied for each year and the even higher number of requests for voluntary disclosure of information, there could be a significant compliance burden associated with such a reporting requirement.

9.67 The international trend towards transparency reporting described above indicates that some organisations that are commonly subject to government requests for data are

---

[50] We note that companies approached to participate in the Privacy Commissioner's trial of transparency reporting said that on average it took half an hour to process a typical request. That figure is the average for all types of requests for information, and is likely to differ significantly depending on the nature and quantity of the information requested. See Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 8.

interested in greater transparency around this sort of activity. That interest appears to stem from a perception that their customers are concerned about:[51]

- whether their personal information is kept private;
- how their information is accessed and used by the government; and
- whether the trade-off of privacy for law enforcement is proportionate.

9.68 We note that in the Privacy Commissioner's report, some of the companies approached to participate in the trial expressed frustration that government agencies did not themselves report on the number of requests for information they made.[52]

9.69 However, we also note that:

- It would perhaps be strange if enforcement agencies were required to report on production orders but not on search warrants, given that production orders were introduced as a less intrusive alternative to search warrants.
- A requirement to report on production orders may provide an unintended incentive for agencies to use other mechanisms to obtain information, such as voluntary disclosure. That risk would, of course, be mitigated if the Act was amended to be clearer about when a production order is required or to require reporting of requests for voluntary disclosure.

Q42 Should enforcement agencies be required to report annually on the number of production orders they have applied for and the outcome of those applications?

## NOTICE REQUIREMENTS

9.70 There is a question for this review about whether the people whose information is disclosed by a third party to an enforcement agency under a production order should be given notice of that disclosure. We note that this issue may apply equally to search warrants.[53] There are two opposing views here. The first view, from a privacy perspective, suggests that the Act should specifically permit the third party to inform their customer of the production order or, alternatively, require the enforcement

---

51 Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 6–7.

52 At 11.

53 As we discuss below at paragraph [9.78], the Act requires a person exercising a search power to provide a copy of the search warrant to the occupier of the place to be searched (or person in charge of the vehicle or other thing to be searched) and an inventory of the items that were seized (ss 131(1) and 133); however, the occupier may not be the person whose items are seized.

agency to inform the person. Under this view, the person whose information is disclosed has a right to know that their information has been accessed so that they can defend their rights if necessary.

9.71 This issue was raised in 2010 when the Search and Surveillance Bill was before the Select Committee. In her submission to the Committee, the (then) Privacy Commissioner argued that enforcement officers should be required to notify the person whose information was obtained that an order was made and the details of the information that was produced. The Committee rejected the idea on the basis that there is no comparable obligation when information is gathered from third parties under a search warrant.[54]

9.72 The second view, from a law enforcement perspective, suggests that the Act should be clearer that the third party must *not* inform the person whose information is disclosed, as that disclosure may prejudice the ongoing criminal investigation.

## Current law

9.73 During our preliminary consultation, it was suggested to us by one agency that the Act already makes it an offence for a third party to disclose the fact of a production order to its customer. Section 179 states:

> (1) No person who, as a consequence of any thing specified in subsection (2), acquires information about any person may knowingly disclose the substance, meaning, or purport of that information, or any part of that information, otherwise than in the performance of that person's duties, functions, or powers.
>
> (2) The things referred to in subsection (1) are—
>
> (a) the exercise of a search or surveillance power:
>
> (b) an examination order:
>
> (c) a production order:
>
> (d) the use of a device, technique, or procedure, or the carrying out of an activity specified in a declaratory order.

9.74 Under a literal interpretation, a third party who discloses the existence of a production order may breach this provision. The "purport" of a production order is that the person whose information is sought is under investigation. By communicating the fact of the production order to that person, the third party would be disclosing that purport (which they acquired as a consequence of the production order) to that person. However, there

---

[54] Search and Surveillance Bill 2010 (45-2) (select committee report) at 12.

are indications that this provision was intended to apply only to enforcement officers and other people within enforcement agencies who acquire the information.

9.75 When the Search and Surveillance Bill (that was ultimately enacted) was introduced in 2009, this provision read:[55]

> No person who, *as a consequence of exercising a search or surveillance power* or as a consequence of assisting another person to exercise a power or carry out an activity of that kind, acquires information about any person may knowingly disclose the substance, meaning, or purport of that information, or any part of that information, otherwise than in the performance of that person's duty.

9.76 The Law Commission and the Ministry of Justice pointed out in their departmental report on the Bill that the clause, as drafted, was limited to people who acquire information when they themselves exercise a search or surveillance power.[56] They considered it should extend to "other people who may have access to such information (eg, a computer technician)".[57] Accordingly, they recommended that the clause be amended so that it is an offence *for anyone to disclose information that is acquired through the exercise of* a search power, surveillance power, an examination order, a production order, or activities carried out under a declaratory order.[58]

9.77 The clause in the Bill was amended accordingly, but the new wording omitted the words "the exercise of", which makes it unclear whether it was intended to extend beyond members of the enforcement agency.

### *Other notification requirements in the Act*

9.78 There are a variety of other notification requirements in the Act. A person exercising a search power must announce their intention to search and provide the occupier of the place searched (or person in charge of the vehicle or thing searched) with a copy of the search warrant and a list of the things that were seized.[59] However, if the information sought relates to a person who is not the occupier, there is no corresponding obligation to notify that other person of the search. If the occupier of the place searched is not

---

55 Search and Surveillance Bill 2009 (45-1), cl 171 (emphasis added).

56 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [612].

57 At [612].

58 At [614].

59 Search and Surveillance Act 2012, ss 131(1) and 133.

present at the time of the search, written notice of the search and things seized must be left at the place.[60] A judge may defer those obligations to provide notice for up to 12 months if providing notice would endanger the safety of a person or prejudice ongoing investigations.[61]

9.79 A person who conducts a remote access search must send an electronic message to the email address of the thing searched, attaching the warrant and setting out particulars of the search.[62] It is only if that message is unable to be delivered that the person conducting the search has an obligation to take all reasonable steps to identify and notify the user of the thing searched.[63] As we discuss in Chapter 6, there is currently no power to defer notice of a remote access search.[64]

## Analysis

9.80 The main advantage of requiring notice to the person whose information is sought under a production order is that it increases transparency and allows the individual to challenge the disclosure if there are grounds to do so. In theory, it may also allow a person to claim any relevant privilege in respect of the information, although we note that notice would probably occur after the production order is executed, rather than before, so any privileged material may have already been seen.

9.81 Conversely, the main disadvantage of notification is that it may prejudice the future law enforcement investigation. This risk is perhaps greater for production orders than for search warrants because they tend to be used at an earlier point in an investigation. For example, if the individual is informed that his or her text messages have been disclosed under a production order, he or she may take steps to hide evidence that might otherwise be found in the execution of a subsequent search warrant. This risk could be mitigated by allowing deferred notification as is permitted under section 134.

9.82 If the Act required the enforcement agency to provide notification, it could be quite time-consuming to identify and notify each of the people for whom information is sought. Delayed notification is likely to be required frequently. In general, we note

---

60 Search and Surveillance Act 2012, s 131(4).

61 Section 134. This power is generally used in relation to covert operations.

62 Section 132(1).

63 Section 132(2).

64 See paragraph [6.109] above.

that it may be more efficient for the third party to provide notification, particularly if they maintain a database of contact information.

Q43 Should the Act require or enable notification to a person whose information is disclosed under a production order?

Q44 If you do not favour notification, should the Act prohibit third parties from disclosing the fact of a production order to the person whose information is sought?

## PRESERVATION ORDERS

9.83 Unlike equivalent legislation in most of the other jurisdictions we compare ourselves to, the Act does not provide a regime under which entities that hold information relevant to criminal investigations can be required to temporarily preserve that information while a search warrant or production order is sought. The type of information often required for law enforcement purposes may not be retained for the business purposes of the network operator. It may be deleted or over-written within days after its creation. Two common examples are telecommunications information (either the content of the communications or the metadata associated with it) and footage from CCTV surveillance. An issue for this review is whether the Act should provide a mechanism for requiring temporary preservation of specified information relating to an investigation while an enforcement officer seeks authorisation to access it.

9.84 Preservation of data is often confused with the retention of data. Preservation refers to a requirement to preserve and maintain the integrity of certain *particularised data* for a temporary period while the enforcement agency seeks authorisation to access it. Retention refers to a requirement to retain certain *types of data* for a fixed period of time so that it may be available if the enforcement agency considers it is necessary for an investigation. Both types of regimes provide merely for the capturing of data. Enforcement agencies must then rely on whatever regime is applicable to access the information, such as a search warrant or production order.

9.85 Currently, the Act does not provide for the preservation of data. A production order only requires a third party to provide documents in their possession or control as at the date of the production order. Any documents deleted or lost before that date are not available for law enforcement purposes.

## Possible problems

### *Access to potential evidence*

9.86 The information sought under a production order is usually personal information stored by a third party service provider. The collection, storage and use of that personal information is governed by the Privacy Act 1993. Information privacy principle nine under that Act limits the timeframe within which personal information can be stored:[65]

> An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

9.87 This means that companies can only keep their customers' personal information for the time it is relevant to their business purposes. They may also frequently over-write data due to limited storage capacity. That may be a shorter period than is required for law enforcement purposes. In practice, some data is deleted within hours or days of its creation, but it may take several days to obtain a production order. By the time a production order comes into force, the relevant information may no longer be stored. While there is provision in the Act to make oral applications for production orders,[66] that procedure is designed for exceptional circumstances only.

9.88 We would be interested to hear feedback on the extent of this problem and how it is being influenced by the changing nature of our use of telecommunications and the changing nature of the industry.

### *Budapest Convention*

9.89 The absence of a regime in the Act for preserving computer data for law enforcement purposes is one of the key reasons New Zealand has not yet acceded to the Budapest Convention,[67] which we described in Chapter 6. Article 16 of the Convention requires States to adopt legislative or other measures to enable law enforcement agencies to order the expeditious preservation for up to 90 days of computer data that is vulnerable to loss or modification. Although a preservation regime in the Act could apply more

---

65 Privacy Act 1993, s 6, principle 9.

66 Search and Surveillance Act 2012, s 100(3).

67 Council of Europe Convention on Cybercrime ETS 185 (opened for signature 23 November 2001, entered into force 1 July 2004) [Budapest Convention].

broadly than to computer data, it would seem that such a regime would remove a key hurdle to New Zealand's accession to the Convention.

9.90 The Government has said that it will consider progressing New Zealand's accession of the Budapest Convention as part of its 2015 cybercrime strategy.[68] The advantages of acceding to this Convention are three-fold:

- it would enhance New Zealand's reputation as a trusted international partner;
- it would provide a platform to enable an expansion of reciprocity arrangements with foreign law enforcement agencies; and
- it would strengthen New Zealand's ability to fight transnational crime.

9.91 These three advantages are inter-related and are demonstrated by way of the example of cross-border searches of digital material. As we described in Chapter 6, often digital material accessed via the Internet is stored on a server located overseas.[69] The only official way to access information located in another jurisdiction is through a process of mutual legal assistance. That process can take months, which is obviously an impediment to the effective investigation and prosecution of crime.

9.92 We also described in that chapter how other jurisdictions have begun negotiations to provide a solution to this problem. The negotiations are aimed at agreeing on new international treaties that would allow law enforcement agencies from one State to issue warrants or orders to communications companies in other States, requiring them to provide access to information for the purposes of investigating crime.[70] The key negotiating hurdle for these treaties is assurance that the powers to issue warrants and orders are subject to adequate protections for the privacy of personal information.

9.93 It is in New Zealand's interests to be party to these negotiations – both from a law enforcement perspective (it would provide more efficient access to data for investigations) and from a privacy perspective (it would provide more assurance that requests for information are subject to strict controls). However, our accession to the Budapest Convention is seen as a key prerequisite to enter these negotiations because

---

[68] Department of Prime Minister and Cabinet "New Zealand's Cyber Security Strategy" (December 2015) <www.dpmc.govt.nz/dpmc/publications/nzcss>. See *National Plan to Address Cybercrime* (2015) at 14.

[69] See paragraph [6.113] above.

[70] Ellen Nakashima and Andrea Peterson "The British Want to Come to America – With Wiretap Orders and Search Warrants" *The Washington Post* (online ed, Washington DC, 4 February 2016).

it would demonstrate that our laws have reached the standard required by that Convention.

## Overseas jurisdictions

### *Canada*

9.94 Canada recently included a preservation regime in its Criminal Code, which enabled it to accede to the Budapest Convention in July 2015. The regime provides for preservation demands and preservation orders, which can apply to any type of computer data.

9.95 A preservation demand may be made by a peace officer or a public officer and requires the specified data to be preserved for 21 days.[71] The enforcement officer making the preservation demand may impose conditions in the demand, including a prohibition on disclosing the existence of the demand or its contents. A preservation order is made by a justice or judge on application by a peace officer or public officer.[72] It requires the specified data to be preserved for 90 days.

### *Australia*

9.96 Australia acceded to the Convention in November 2012. The Cybercrime Legislation Amendment Act 2012 was passed for the purpose of implementing that Convention. It provides a preservation regime in respect of telecommunications data only. Under that regime, a law enforcement agency may give a preservation notice to a telecommunications provider that is in force for 90 days.[73] We have heard that preservation notices have never been used in Australia. If that is correct, it is likely to be because telecommunications providers in that country are also subject to requirements to retain certain metadata for two years.[74]

---

71 Criminal Code RSC 1985 c C-46, s 487.012. The Code defines "peace officer" and "public officer" as including a wide range of people, such as mayors, sheriffs, members of the Correctional Service, police officers and bailiffs.

72 Criminal Code RSC 1985 c C-46, s 487.013. If the offence in question was committed in a foreign State, the justice or judge must also be satisfied that a person or authority with responsibility in that State for the investigation of such offences is conducting the investigation.

73 Telecommunications (Interception and Access) Act 1979 (Cth), ss 107H–107K (as amended by the Cybercrime Legislation Amendment Act 2012 (Cth)).

74 Telecommunications (Interception and Access) Act 1979 (Cth), s 187C.

### *United Kingdom*

9.97 The United Kingdom signed the Convention in 2001 and ratified it in May 2011. It does not have a regime for preservation orders in its domestic legislation because it has a data retention regime instead. Under the Data Retention and Investigatory Powers Act 2014 (UK) (DRIPA), telecommunications operators can be required to retain communications data for up to 12 months. In November 2015, the United Kingdom Government introduced the Investigatory Powers Bill, designed to consolidate the powers in DRIPA and two other statutes regulating telecommunications. That Bill is currently under consideration by the House of Lords.

## Options for reform

9.98 The Act could be amended to include a preservation regime if the deletion of data in the ordinary course of business is impeding effective law enforcement, or if New Zealand wishes to accede to the Budapest Convention. We wish to hear submitters' views on whether the current inability to require preservation of data has been causing problems in practice.

9.99 There are a number of options for framing the scope of a preservation regime. To date, we have done little analysis of the implications of these various options. We mention them here to seek feedback and to give a sense of the questions that would need to be resolved.

### *Type of data holder*

9.100 There are a variety of options for defining who may be subject to a preservation request. It could be as broad as a production order – "any person" could be requested to retain information.

9.101 Alternatively, it could follow the Australian model and be confined to telecommunications providers on the basis that telecommunications data is particularly vulnerable to deletion or modification. Within the telecommunications industry, it could be limited to retail providers because they hold the vast bulk of relevant data and wholesalers are merely the conduit for communications to the retail sector. Telecommunications data is of special interest because of its unique value for the investigation of offences, the fact that searches of it can be highly intrusive of privacy and because compliance with any preservation regime would presumably require significant investment and infrastructure on the part of telecommunications providers.

9.102 Any proposal for a preservation regime would need to have considered the compliance costs for the relevant data holders.

### *Types of data*

9.103 A preservation regime could either define the type of data that may be subject to a preservation request or it could build that into the threshold test. For example, the provision could state that a request to preserve data may only be made if the person making the request has reasonable grounds to believe that the data will be lost before an application for a warrant or production order can be determined.

9.104 In respect of telecommunications data, it is likely that a preservation regime would need to include both content and metadata.

9.105 Additionally, any preservation regime should be clear that the requirement is only to preserve documents that are already stored in the normal course of business. An obligation to store a certain type of data in case it is required in the future is, in effect, a retention regime.[75] This is not required under the Budapest Convention and is not being considered in this review.

9.106 It is noted that, while the obligation to preserve documents would only apply in respect of data already stored in the normal course of business, it is likely that some businesses would need to adapt their systems to enable them to extract and store the specific data requested for the duration of the order.

### *Issuing entity*

9.107 The two options for who might have authority to issue a preservation request appear to be either the enforcement agency that wishes the data to be preserved or an issuing officer under the Act. We note that the Australian legislation permits the law enforcement agency to issue a preservation notice.[76] However, as mentioned, the Canadian legislation has separate regimes for:[77]

- a "preservation demand" issued by a peace officer or public officer for only 21 days; and

---

[75] We described the difference between a preservation regime and a retention regime above at paragraph [9.84].

[76] Telecommunications (Interception and Access) Act 1979 (Cth), s 107H (as amended by the Cybercrime Legislation Amendment Act 2012 (Cth)).

[77] Criminal Code RSC 1985 c C-46, ss 487.012 and 487.013.

- a "preservation order" issued by a justice or a judge for 90 days.

9.108 We can immediately see two disadvantages to requiring preservation orders to be made by issuing officers. First, if the purpose of a preservation regime is to ensure that data is not lost while a production order or search warrant is applied for, it would seem to defeat that purpose to require an application to be made to an issuing officer. Any such application is likely to take almost as long as applying for a production order. Second, given that preservation does not authorise an agency to access the data (it merely preserves it), there may be insufficient justification to impose this administrative burden and extra cost on both enforcement agencies and the court system.

### *Threshold for a preservation request*

9.109 The Budapest Convention does not address the appropriate threshold for issuing a preservation order, although it states that the requirement for a preservation regime is particularly relevant "where there are grounds to believe the computer data is particularly vulnerable to loss or modification".[78] There are a variety of options for framing this threshold. One option is for the threshold to be the same as for a production order, meaning that there must be:

- reasonable grounds to suspect that a relevant offence has been, is being, or will be committed; and
- reasonable grounds to believe that the documents specified will constitute evidential material in respect of that offence and will be in the possession or control of the person subject to the request at the time it is made.

9.110 This may be considered to be appropriate if the purpose of preservation orders is to ensure that the data is not deleted while the enforcement agency applies for a search warrant or a production order.

9.111 However, it may be thought that a slightly lower threshold is appropriate, given the enforcement agency may need more time to gather all the evidence required to meet the grounds for a production order or search warrant. We note that the Canadian threshold for a preservation demand or preservation order only requires "reasonable grounds to suspect" that the computer data is in the person's possession or control,

---

[78] Budapest Convention, above n 67, art 16.1.

rather than "reasonable grounds to believe" as is required for a search warrant in New Zealand.[79] Also, the Canadian thresholds only require the computer data to "assist in the investigation of the offence", rather than "constitute evidential material", as is required in New Zealand. Similarly, the Australian thresholds only require "reasonable grounds to suspect" that the data exists and "might assist in connection with the investigation".[80]

### *Duration of preservation*

9.112 The Budapest Convention requires that any preservation regime provides for computer data to be preserved for up to 90 days. As already mentioned, the Australian and Canadian regimes also provide for preservation notices to be in force for 90 days (or in Canada, for only 21 days if the demand is made by the enforcement agency).[81] Subject to feedback from enforcement agencies as to the adequacy of that time period for law enforcement purposes, we doubt there would be reasons to extend the requirement beyond the time period set out in the Convention.

### *Prospective preservation requests*

9.113 Currently, a production order may require a person to either produce a document on one occasion or to produce a type of document on an ongoing basis for the duration of the order.[82] A preservation regime could similarly target either documents already in the possession or control of the person (retrospective preservation) or any documents that will come into the person's possession or control (prospective preservation). In either case, the data would be held for up to 90 days or for whatever maximum period is specified in the Act.

9.114 The Budapest Convention does not require prospective preservation but the Australian legislation provides for it, nonetheless.[83] The main advantage of allowing for

---

79 Criminal Code RSC 1985 c C-46, ss 487.012(2)(c) and 487.013(2)(a). We note that there is an additional condition relevant only when the offence is committed under a law of a foreign State. Also, when a justice or judge is making the determination, he or she must also be satisfied that a peace officer or public officer intends to apply or has applied for a warrant or an order in connection with the investigation to obtain a document that contains the computer data.

80 Telecommunications (Interception and Access) Act 1979 (Cth), s 107J.

81 Telecommunications (Interception and Access) Act 1979 (Cth), s 107K; Criminal Code RSC 1985 c C-46, ss 487.012 and 487.013.

82 Search and Surveillance Act 2012, s 71(2)(g).

83 Telecommunications (Interception and Access) Act 1979 (Cth), s 107H(1)(b)(ii).

prospective preservation (besides the advantage of aligning with the production order regime) is likely to be that it avoids the need for enforcement officers to make multiple preservation requests (or apply for multiple preservation orders).

9.115 If requests for prospective preservation were permitted, the Act would need to specify the time period in which that request applied. We note that production orders can be in force for 30 days. It may be that a similar time period is appropriate.

Q45 Is there a problem with data being unavailable by the time enforcement agencies have obtained a search warrant or production order?

Q46 Should the Act be amended to include a preservation regime? If so, do you have views on the design of that scheme?

# Chapter 10 – Examination orders

## INTRODUCTION

The examination order regime in the Search and Surveillance Act 2012 (the Act) provides a power—available only to New Zealand Police—to obtain a court order requiring a person to submit to compulsory questioning. Since the Act's enactment, the examination order regime has yet to be employed by Police.

Examination orders were one of the most contentious aspects of the Search and Surveillance Bill and were the subject of considerable debate in the House.[1] Concern was raised that they would remove an individual's right to silence and the privilege against self-incrimination.[2]

The main issue arising in this review in relation to examination orders is whether—given they have not been used—there is a continuing need for the regime.

## OVERVIEW OF THE EXAMINATION ORDER REGIME

### What is an examination order?

Under the Act, Police may obtain an examination order from a judge[3] to require a person to answer questions in relation to identified information, where he or she has previously refused to do so.[4]

An examination order may be made in either a "business" or "non-business" context. Those terms are defined in section 3.[5] In short, examination orders in a business context are directed at persons who hold information in a professional capacity that they do not want to disclose voluntarily. In a non-business context, examination orders may be directed to any person who holds information that he or she does not wish to disclose.

---

1 Search and Surveillance Bill 2010 (45-2) (select committee report) at 8.

2 At 8.

3 Section 3 of the Search and Surveillance Act 2012 defines "Judge" as a District Court judge or a judge of the High Court.

4 Search and Surveillance Act 2012, ss 33–43.

5 "Business context," in relation to the acquisition of any information by a person, means the acquisition of the information in the person's capacity as — (a) a provider of professional services or professional advice in relation to a person who is being investigated, or one or more of whose transactions are being investigated, in respect of an offence; or (b) a director, manager, officer, trustee, or employee of an entity that is being investigated, or one or more of whose transactions are being investigated, in respect of an offence. "Non-business context" means a context other than a business context.

There are a number of procedural and substantive hurdles that need to be overcome before Police can obtain an examination order.

### *Procedural requirements*

An application for an examination order may only be made by a Police Inspector or more senior officer, and must be approved by the Police Deputy Commissioner, Assistant Commissioner, or District Commander.[6]

The Commissioner of Police or a delegate of the Commissioner must conduct the examination[7] and provide a formal report to the issuing judge within one month.[8]

### *Substantive requirements*

Examination orders are available only where there are reasonable grounds to suspect that an offence has been, is being, or will be committed.[9] The orders may only be made in relation to sufficiently serious suspected offences. How serious the offence needs to be depends on whether the order is made in a business or non-business context:

- in a business context, an examination order may only be made if the offence in question is punishable by five years' imprisonment or more;[10] and
- in a non-business context, the offence must be serious or complex fraud punishable by seven years' imprisonment or more, or an offence committed by an organised criminal group.[11]

In both cases, there must also be reasonable grounds to believe that the person to be examined (the examinee) has information that constitutes evidential material in respect

---

6 Search and Surveillance Act 2012, ss 33(1) and 35(1).

7 Section 39(1).

8 Section 43. The report must address whether the examination resulted in obtaining evidential material; whether any criminal proceedings have been brought or are under consideration as a result of evidential material obtained by means of the examination; and any other information stated in the order as being required for inclusion in the examination order report (s 43(2)). The Police annual report must also include the number of examination orders that were granted or refused in that year (s 170(1)(c)).

9 Sections 34(a) and 36(a).

10 Section 34(a).

11 Section 36(a). The definition of "organised criminal group" in s 98A(2) of the Crimes Act 1961 applies to this section.

of the offence, and the examinee must have declined to provide the information despite being given a reasonable opportunity to do so.[12]

The issuing judge must also be satisfied that it is reasonable to subject the examinee to compulsory examination, having regard to the nature and seriousness of the suspected offending, the nature of the information sought, the relationship between the examinee and the suspect, and any alternative ways of obtaining the information.[13]

### *The examination process*

Once an examination order has been issued, the examinee must be given a reasonable opportunity to arrange for a lawyer to be present during the examination.[14] The examinee may refuse to answer a question by invoking the privilege against self-incrimination,[15] or any other privilege recognised under the Act.[16] If the examinee refuses to answer a question on the grounds of privilege, the Commissioner may apply to a judge for an order determining whether the claim is valid.[17]

It is an offence to fail to comply with an examination order without reasonable excuse.[18] The maximum penalty is one year's imprisonment (in the case of an individual) or a $40,000 fine (in the case of a body corporate).

## Genesis of the examination order regime

Examination orders were not included in the Law Commission's 2007 Report, *Search and Surveillance Powers*.[19] They were beyond the Commission's terms of reference. The examination order regime was developed at a later point, when the Government was considering the implementation of the Commission's Report. In September 2007, the Labour Government announced its plans to set up an Organised Financial Crime Agency within Police and to disestablish the Serious Fraud Office (SFO). It was proposed that SFO's functions would be integrated into those of the new agency,

---

12 Search and Surveillance Act 2012, ss 34(d) and 36(d).

13 Section 38(b).

14 Section 40.

15 Section 138(1).

16 Section 139(1).

17 Sections 138(3) and 139(2).

18 Section 173.

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

which would have the same investigative tools and powers that were available to SFO. One of those powers was SFO's ability to require persons to answer questions relevant to an investigation into serious or complex fraud.[20] (SFO's examination powers are discussed later in this chapter.[21])

Accordingly, a Police-only examination order was included in the Search and Surveillance Powers Bill, introduced by the Labour Government in September 2008.[22] That Bill was subsequently discharged.

In July 2009, the National Government decided not to integrate SFO into Police, but nonetheless retained the examination order regime in the Search and Surveillance Bill 2009 (which was ultimately enacted).

## The rationale for examination orders

During the Bill's passage, the complex nature of fraud offending was suggested as a reason why special examination powers were needed.[23] It was suggested that investigations of offending involving complex financial transactions could benefit from a power requiring a person to answer questions about complicated documents and paper trails (already obtained by Police) relating to these transactions.[24] Access to pre-existing documents would not always give the investigator a clear picture of what had occurred; so it was thought that the investigation of fraud could be carried out more effectively if persons with relevant information could be compulsorily examined.

It was also suggested that examination orders could assist in situations where a person was reluctant to assist Police on the grounds of professional confidentiality.[25] In a business context, a person may acquire information in the course of providing professional services and not wish to disclose this information because of professional or fiduciary obligations owed to the client. For example, chartered accountants have an obligation to respect the confidentiality of information about their clients' affairs (set out in the New Zealand Institute of Chartered Accountants' code of ethics) and may

---

20 Serious Fraud Office Act 1990, s 9(1)(d).

21 See paragraphs [0]–[0] below.

22 Search and Surveillance Powers Bill 2008 (300-1), cls 33 and 35.

23 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [164]; (1 March 2012) 677 NZPD 761; Search and Surveillance Bill 2010 (45-2) (select committee report) at 8.

24 Ministry of Justice and Law Commission *Departmental Report*, above n 23, at [164].

25 Search and Surveillance Bill 2010 (45-2) (select committee report) at 8–9.

fear disciplinary action for breaching the Institute's code if they voluntarily disclose this information to Police. Compulsory questioning would allow such persons to cooperate with Police without fear of adverse legal or ethical consequences (whether real or perceived).[26]

In the case of persons who have obtained information about suspected offending in a non-business context, the information will generally have come into their knowledge through a personal relationship with the suspect. There are many reasons why a person may be reluctant to disclose that information to the Police voluntarily (for example, fear of jeopardising social relationships). Cooperating with Police could have serious and ongoing consequences, given the more enduring nature of personal relationships compared to business relationships.[27] The Select Committee was concerned that compulsory questioning would adversely affect personal relationships, but ultimately considered this was justified to help Police unravel complex transactions and arrangements when investigating serious financial crime and organised crime.[28]

## The right to silence

Because examination orders compel a person to submit to police questioning, concerns were raised during the Bill's passage that they infringed the general right held by all citizens to remain silent and to decline to provide information.[29]

The "right to silence" has been described as a network of loosely linked rules or principles of immunity, differing in scope and rationale.[30] Broadly speaking, these rules reflect the principle that "every citizen has in general a right to refuse to answer questions from anyone, including an official".[31] The right may be seen as an essential

---

26 Search and Surveillance Bill 2010 (45-2) (select committee report) at 8–9; Ministry of Justice and Law Commission *Departmental Report*, above n 23, at [170].

27 Search and Surveillance Bill 2010 (45-2) (select committee report) at 9; Ministry of Justice and Law Commission *Departmental Report*, above n 23, at [171].

28 Search and Surveillance Bill 2010 (45-2) (select committee report) at 8.

29 Search and Surveillance Bill 2010 (45-2) (select committee report) at 8; and see the submissions referred to in Ministry of Justice and Law Commission *Departmental Report*, above n 23, at [159].

30 *R v Hertfordshire County Council* [2000] 2 AC 412 (HL) at 419, referring to *R v Director of Serious Fraud Office, ex parte Smith* [1993] AC 1 (HL) at 30–31. The right to silence is discussed in Law Commission *Criminal Evidence: Police Questioning* (NZLC PP21, 1992) at 10–26.

31 *Taylor v New Zealand Poultry Board* [1984] 1 NZLR 394 (CA) at 398 per Cooke P. See also *Rice v Connolly* [1966] 2 QB 414 at 419: "the whole basis of the common law is the right of the individual to refuse to answer questions put to him by persons in authority".

component of a citizen's "right to be let alone"[32] and to be free from unwarranted State intrusion into his or her private life.[33]

In New Zealand, the general right to silence is not subject to explicit legislative protection. However, specific instances of the right are given special protection. For example:

- section 23(4) of the New Zealand Bill of Rights Act 1990 (NZBORA) guarantees the right to silence when a person has been arrested or detained;
- section 25(d) of NZBORA guarantees the right not to be compelled to be a witness or confess guilt at trial; and
- section 60 of the Evidence Act 2006 preserves the common law immunity against being compelled to answer any questions that may incriminate oneself (known as the "privilege against self-incrimination").

The Select Committee acknowledged submitters' concern that examination orders would remove an individual's right to silence, but concluded there were strong policy reasons for the examination order regime to remain in the Bill.[34] The Committee also noted that the Bill expressly preserved the examinee's privilege against self-incrimination; and that the proposed use of examination orders would be subject to more rigorous scrutiny than under the Serious Fraud Office Act 1990 (as examination orders would require prior judicial authorisation).[35]

The Committee did, however, recommend a number of amendments to ensure that examination orders would not become a routine tool for investigation. These amendments (which were carried through into the final Act) included raising the threshold for issuing examination orders,[36] creating an internal oversight process for making applications,[37] and strengthening reporting requirements.[38]

---

32 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [10] per Elias CJ, referring to *Olmstead v United States* 277 US 438 (1928) at 478 per Brandeis J and *Katz v United States* 389 US 347 (1967) at 350 per Stewart J.

33 See Law Commission *Criminal Evidence: Police Questioning* (NZLC PP21, 1992) at 23.

34 Search and Surveillance Bill 2010 (45-2) (select committee report) at 8. This was the view of the majority of the Select Committee. The minority views of the Green Party and Labour Party, who were opposed to the provisions relating to examination orders, are recorded at 21–25 of the final Select Committee report.

35 Search and Surveillance Bill 2010 (45-2) (select committee report) at 9.

36 The Bill as introduced provided that examination orders were available for information obtained: in a business context, in relation to investigations of *any* imprisonable offence; and in a non-business context, in relation to investigations of *any* imprisonable offence that was serious or complex fraud or committed because of participation in a continuing association of

## EXAMINATION POWERS IN OTHER ACTS

Examination orders under the Act were an entirely new power for Police in the investigation of suspected criminal offending. However, the concept and use of examination powers was not novel. There are similar powers in other statutes that permit government bodies to submit people to compulsory questioning. Some of those examination powers are briefly described below.

### Serious Fraud Office Act 1990

As mentioned above, there is an examination power available to SFO to require persons to answer questions in the investigation of suspected serious or complex fraud.[39] The Director of SFO must have reasonable grounds to believe that an offence involving serious or complex fraud may have been committed before using this power.[40]

The examination power may be exercised by the Director giving notice in writing to the examinee[41] (rather than requiring a judicial order) and remains unaffected by the enactment of the Search and Surveillance Act. The examinee may be either the person whose affairs are being investigated by SFO or any other person whom the Director

---

three or more persons (having a continuing course of criminal conduct as one of its objects). The Select Committee recommended limiting examination orders in the business context to offences punishable by five years' imprisonment or more; and, in the non-business context, to serious or complex fraud offences punishable by seven years' imprisonment or more, or offences committed by an "organised criminal group" as defined in s 98A(2) of the Crimes Act 1961.

37 The Select Committee recommended that only police officers holding the rank of Inspector or higher could make an examination order and applications would need to be approved by a Deputy Commissioner, Assistant Commissioner or District Commander.

38 The Select Committee recommended imposing reporting requirements on police officers questioning people under examination orders and through the Police's annual report to Parliament.

39 "Serious or complex fraud" is defined in s 2 of the Serious Fraud Office Act 1990 as including "a series of connected incidents of fraud which, if taken together, amount to serious or complex fraud". When determining whether suspected offending involves serious or complex fraud, the Director may have regard to the nature and consequences of the fraud; the scale of the fraud; the legal, factual and evidential complexity of the matter; and any relevant public interest considerations (s 8(d)). The Serious Fraud Office (SFO) can assume responsibility from Police for investigating any case the Director believes on reasonable grounds to involve serious or complex fraud (s 11(1)(a)). If a complaint of fraud does not meet the criteria required for SFO investigation, SFO may direct complainants to another law enforcement agency, or refer the matter to that agency itself.

40 Serious Fraud Office Act 1990, s 7.

41 Section 9(1).

has reason to believe may have information or documents relevant to an investigation.[42] Failure to answer a question during examination is an offence.[43]

In contrast to the Search and Surveillance Act, the Serious Fraud Office Act expressly removes the privilege against self-incrimination. Section 27 provides:

> **Privilege against self-incrimination no excuse**
>
> No person shall be excused from answering any question, supplying any information, producing any document, or providing any document, or providing any explanation pursuant to section 5 or section 9 of this Act on the ground that to do so would or might incriminate or tend to incriminate that person.

Although the privilege against self-incrimination is removed, section 28(1) of the Serious Fraud Office Act provides that a self-incriminating statement can only be used in evidence against that person in a prosecution for an offence if he or she gives evidence inconsistent with the statement.

## Insolvency Act 2006

Under the Insolvency Act 2006, the Official Assignee has the power to summons certain persons for questioning on oath in relation to the property and transactions of a bankrupt.[44] Like the Serious Fraud Office Act, there is nothing to preclude questions that may elicit self-incriminating answers.[45] However, such statements cannot be used in criminal proceedings against that person unless he or she is charged with perjury in relation to the statement.[46]

## Criminal Proceeds (Recovery) Act 2009

The Criminal Proceeds (Recovery) Act 2009 establishes a regime for the forfeiture of the proceeds of crime in New Zealand.[47] Under that Act, the Commissioner of Police may apply to a High Court judge for an examination order.[48] Section 107 empowers a judge to make an order requiring a person to attend before the Commissioner and

---

42 Serious Fraud Office Act 1990, s 9(1)(a)–(b).

43 Section 45(d)(ii). The maximum penalty in the case of an individual is one year's imprisonment or a $15,000 fine; and, in the case of a corporation, a $40,000 fine.

44 Insolvency Act 2006, s 165(1).

45 Section 184(2).

46 Section 185(2)(a). Or, in the case of the bankrupt, if the bankrupt is charged with making a misleading statement: s 185(2)(b).

47 It replaces the Proceeds of Crime Act 1991.

48 Criminal Proceeds (Recovery) Act 2009, s 106.

answer questions in relation to any matter that the Commissioner has reason to believe may be relevant to the investigation or to any proceedings under the Act. The order may be made if the judge is satisfied that the Commissioner has reasonable grounds to apply for the examination order.[49] Failure to comply with an examination order is an offence.[50]

Like the Serious Fraud Office Act, the Criminal Proceeds (Recovery) Act removes the privilege against self-incrimination,[51] but there are restrictions on the ability to use self-incriminating statements obtained during the examination process in criminal proceedings.[52]

## CURRENT PRACTICE

Police have not yet applied for any examination orders under the Search and Surveillance Act.[53] In contrast, SFO used its examination powers on 32 occasions in 2014, 64 occasions in 2013, and 73 occasions in 2012.[54]

Police told us that they have not used the examination order regime in the Search and Surveillance Act because they do not tend to investigate many serious or complex fraud cases.[55] Most serious or complex fraud investigations are conducted by SFO.

Police also told us that some of their investigations could have benefited from the use of examination orders, but this did not occur because of knowledge gaps within the police force about their availability.

## ISSUES FOR CONSIDERATION

The main issue arising in this review in respect of examination orders is whether—because they have not yet been employed by Police—they should remain in the Act.

---

49 Criminal Proceeds (Recovery) Act 2009, s 107(1).

50 Section 152(1)(a). The maximum penalty in the case of an individual is one year's imprisonment or a $15,000 fine; and, in the case of a body corporate, a $40,000 fine.

51 Section 163.

52 Section 165, which provides that any self-incriminating statement may be used in evidence against that person only in a prosecution for perjury, or in relation to any evidence given by the person that is inconsistent with the statement.

53 According to the Police annual reports, since 1 October 2012 no applications for examination orders have been made, granted or refused.

54 See Serious Fraud Office "Annual Reports" <www.sfo.govt.nz/annual-reports>.

55 The Auckland City Police District has a dedicated Financial Crime Unit that investigates fraud (some of these investigations involve serious or complex fraud), but other districts do not have dedicated fraud units.

Another issue we discuss in this chapter is whether the Act should be clearer about who can be an examinee (namely whether persons suspected of, arrested for, or charged with the offending in question should be subject to compulsory examination). Issues concerning the interaction of the examination order regime with claims of privilege were dealt with in Chapter 8.

## Is there a problem with retaining the examination order regime in the Act?

We welcome comments on whether there are any problems with retaining the examination order regime in the Act.

On one hand, the regime arguably provides Police with a valuable investigative tool in relation to certain serious offences. Although examination orders have not yet been used, there may be future occasions where the investigation of complicated financial transactions can be carried out more effectively if people with relevant information can be required to answer questions.[56] Our understanding is that Police intend to provide further guidance and education to staff on the availability and use of examination orders.[57]

Moreover, although examination orders are a coercive tool available to Police in the investigation of suspected criminal offending, the Act imposes a number of safeguards and limitations surrounding their use. In particular:

- Judicial approval of an examination order is required before Police can subject a person to compulsory examination. In contrast, SFO can exercise its examination powers simply by issuing a notice to the person to be examined.
- The privilege against self-incrimination is expressly preserved in the Act. This means that an examinee can refuse to answer questions if the answer is likely to incriminate him or her. In contrast, the privilege is removed under the Serious Fraud Office Act, Insolvency Act and Criminal Proceeds (Recovery) Act. Under these Acts, there is nothing to stop a question being asked during examination that

---

[56] For example, we understand that examination orders may be useful in the context of investigating money laundering, terrorist financing and other serious offences, which may be prompted by suspicious transaction reports made to the Commissioner of Police (under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, which came into force on 30 June 2013).

[57] For example, Police's Financial Crime Group is in the process of establishing and trialling a financial investigation team to support criminal investigations and target facilitators of financial crime.

may elicit a self-incriminating statement (although there are limitations on using those statements in subsequent criminal proceedings).

Further, police practice since the Act came into force demonstrates that one of the principal concerns during the Bill's passage—that examination orders would be used too readily by Police—has not come to pass. Examination orders have not been employed as a substitute for normal police investigative practice.

We also note that if the regime was removed, this might create an anomaly in the powers available to Police and SFO when investigating similar offending. SFO exercises discretion when determining whether to investigate a complaint of fraud.[58] Its current priorities lie with cases involving multiple victims, losses of more than $2 million, and transactions with significant legal or financial complexity.[59] If SFO decides not to pursue an investigation, it may refer the case to another agency (for example, Police). It may be anomalous for an examination power to be available to SFO but not to Police when investigating serious or complex fraud falling just short of the criteria required for SFO investigation.

On the other hand, the lack of use of examination orders under the Act perhaps suggests there is no real practical need for the regime. We note that SFO appears to rely far more heavily on its powers to compel individuals to supply pre-existing documents than it does on its powers to require answers to questions.[60] This perhaps suggests that in practice, documents obtained during an investigation often provide a sufficiently clear picture of offending, without the need to compel persons to answer questions and explain complex documents.

Q47 Should the examination order regime remain in the Act?

---

58 Serious Fraud Office Act 1990, s 8.

59 See Serious Fraud Office "FAQs" <www.sfo.govt.nz/faqs>.

60 According to SFO's annual reports, it used its statutory power to require documents to be produced (under s 9(1)(f) of the Serious Fraud Office Act 1990) on 341 occasions in 2014, 361 occasions in 2013, and 620 occasions in 2012. In contrast, it required compulsory answers on 32 occasions in 2014, 64 occasions in 2013, and 73 occasions in 2012.

## Who can be an examinee?

The Act is not clear as to whether an examination order in a non-business context can be made against a person suspected of, arrested for, or charged with the offending in question.[61]

Section 38 of the Act provides that one of the factors to be considered by the issuing judge when deciding whether to make an examination order is "the relationship between the person to be examined and the suspect".[62] While it may be inferred that a suspect cannot be an examinee, this is not explicit.

In contrast, the Serious Fraud Office Act expressly provides that the Director of SFO may examine "any person whose affairs are being investigated".[63] There is also case law establishing that SFO's examination power may be used against a person who has been charged.[64]

There is no direct discussion in the legislative history of the Search and Surveillance Bill as to whether a suspect can be an examinee. The issue was briefly discussed in relation to production orders in the Law Commission's 2007 Report. The Commission said:[65]

> We have concluded that the issue of production orders where the person to whom the order is directed may be a suspect or the target of the investigation should not be expressly restricted. The person to whom an order is directed should be obliged to produce the items or documents specified. However, if producing the material referred to would be likely to incriminate that person in terms of section 60(1) of the Evidence Act 2006, his or her non-compliance with the order should be justified by the privilege against self-incrimination.

However, in the departmental report provided to the Select Committee, it appears to have been assumed that examination orders could only be obtained "in relation to a person who is not a suspect".[66]

---

61 It appears, however, that examination orders are not available in respect of such persons in a business context because the order must be directed to a person who acquired information in a professional capacity *from the person under investigation*: see the definition of "business context" in s 3 of the Search and Surveillance Act 2012.

62 Search and Surveillance Act 2012, s 38(1).

63 Serious Fraud Office Act 1990, s 9(1)(a).

64 *R v H (No 2)* [1995] DCR 772 (this is the case even if the charges are less serious than those that justified the use of the power under the Serious Fraud Office Act 1990).

65 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.32].

66 Ministry of Justice and Law Commission *Departmental Report*, above n 23, at [201].

Section 23(4) of NZBORA guarantees the right to refrain from making a statement to any person who has been "arrested or detained" under any enactment for any offence or suspected offence. Compulsory examination of persons suspected of, arrested for, or charged with the offending in question may infringe this right, because:

- *Suspects and persons who have been charged:* a person required by statute to attend an examination is arguably detained for the purposes of NZBORA.[67] Persons who are suspected of or charged with the offending in question could be regarded as being detained "for … [a] suspected offence"[68] and may be entitled to refrain from answering questions by virtue of section 23(4).[69]
- *Persons arrested*: a person who is arrested for a suspected offence may refuse to answer questions by virtue of section 23(4).

Any intrusion on the section 23(4) right must be justified on policy grounds, and should be expressly provided in the Search and Surveillance Act. Our (very preliminary) view is that there is no policy justification for Police to subject a person suspected of, arrested for, or charged with the offending in question to compulsory examination. If that is the case, there may be merit in expressly stating in the Act that such persons cannot be subject to an examination order.

Q48 Should examination orders be available in respect of persons suspected of, arrested for, or charged with the offending?

---

67 See *Official Assignee v Murphy* [1993] 3 NZLR 62 (HC) and *Police v Smith and Herewini* [1994] 2 NZLR 306 (CA).

68 New Zealand Bill of Rights Act 1990, s 23(4).

69 *Official Assignee v Murphy*, above n 67, at 72. See also *Police v Smith and Herewini*, above n 67, at 316 and *Commissioner of Police v Burgess* [2016] NZHC 267 at [46].

# Chapter 11 – The use of intelligence agencies' capabilities for law enforcement purposes

## INTRODUCTION

11.1 Earlier this year, the report of the first Independent Review of Intelligence and Security was tabled in Parliament.[1] That review, which was carried out by Sir Michael Cullen and Dame Patsy Reddy, considered the legislation that governs the activities of the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS). The New Zealand Intelligence and Security Bill 2016 has now been introduced to Parliament in response to the recommendations in the Cullen/Reddy report.[2]

11.2 One of the issues considered in the Cullen/Reddy report was the ability of GCSB and NZSIS to assist other government agencies. GCSB has an express function under its legislation of assisting New Zealand Police to perform its functions (that is, law enforcement functions).[3] When doing this, GCSB must act within the scope of police powers. The report recommended that NZSIS should have an equivalent function,[4] which is reflected in the Bill.[5]

11.3 The report also raised, but did not resolve, the question of whether the capabilities of GCSB and NZSIS should be available to assist in the performance of police functions, *outside the scope of current police powers*.[6] The Bill does not make any changes in this regard.[7] Because this would effectively increase the scope of what Police can do, the report suggested it be considered as part of this review of the Search and

---

1 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).

2 The New Zealand Intelligence and Security Bill 2016 (158-1) was introduced and had its first reading in August 2016. At the time of this Issues Paper it is with the Foreign Affairs, Defence and Trade Select Committee, which is due to report back on 18 February 2017. The Bill can be accessed at <www.legislation.govt.nz>.

3 Government Communications Security Bureau Act 2003, s 8C.

4 Cullen and Reddy *Intelligence and Security in a Free Society*, above n 1, at [5.57] and recommendation 29.

5 New Zealand Intelligence and Security Bill 2016 (158-1), cl 16.

6 Cullen and Reddy *Intelligence and Security in a Free Society*, above n 1, at [5.59].

7 Under the Bill, both GCSB and NZSIS would be required to act within the scope of police powers when exercising their assistance function: New Zealand Intelligence and Security Bill 2016 (158-1), cl 16(2).

Surveillance Act 2012 (the Act). That is why this issue was included in our terms of reference.

11.4 Our preliminary view is that the answer to the question above is "no". We see no justification for allowing the capabilities of GCSB and/or NZSIS to be used for law enforcement purposes in a way that goes beyond what Police can (under the current law) lawfully do itself. We also note that neither Police nor the intelligence agencies support such a change. While Police consider that greater assistance from the intelligence agencies might be useful in some cases, the barriers to this occurring are primarily practical rather than legislative.

11.5 However, in order to facilitate informed public debate on this issue, we analyse in this chapter how such a change could work in practice.

11.6 As we understand it, the crux of the issue identified by the Cullen/Reddy report is that, because GCSB must act within the scope of police powers under the Act when assisting in the performance of police functions, it cannot use its capabilities to detect crime at an early stage. Instead, it can only assist where the criteria for a warrant or search power under the Act are met. This generally requires reasonable grounds to suspect the commission of an offence and belief that the search or surveillance will find evidential material relating to that offence.

11.7 We have identified two possible ways in which this issue could, theoretically, be addressed:

- the legislation governing GCSB and NZSIS could be amended to give those agencies an explicit function of contributing to the prevention and detection of crime; or
- the Act could be amended to allow search and surveillance activities (either by Police, or by GCSB or NZSIS when providing assistance) to be carried out before the point at which reasonable belief is established.

11.8 In the discussion that follows we explain how the intelligence agencies can assist or cooperate with Police under the current law and explore the implications of the two possible changes identified above. We express our preliminary view that neither of these changes is likely to be necessary or justified, and seek submitters' views on this.

## THE CURRENT LAW

11.9 In this section, we briefly summarise the functions and powers of GCSB and NZSIS, compare those to the powers of Police under the Act, and explain the current scope of

GCSB and NZSIS's ability to assist law enforcement agencies. This description is based on the current law. While some aspects of the law may change if the New Zealand Intelligence and Security Bill is passed, the functions and powers of NZSIS and GCSB discussed below will remain broadly similar (except where otherwise noted).

11.10 The comparison below suggests that there is no significant gap in the legal ability of GCSB to assist Police where a specific crime is being investigated and where a warrant can be obtained (or a search power can be exercised) under the Act.[8] It appears that the main area where there may be scope for increased intelligence agency support for police investigations is at the point of preventing or detecting crime rather than investigating specific offending.

## The functions and powers of GCSB and NZSIS

### *GCSB*

11.11 GCSB's current functions are to:

- provide advice and assistance relating to cyber security and the protection of communications and information infrastructures;[9]
- collect and analyse intelligence about the capabilities, intentions and activities of foreign persons or organisations;[10] and
- assist Police, the New Zealand Defence Force and NZSIS to perform their functions.[11]

11.12 As a foreign intelligence agency, GCSB collects information that will help to advance New Zealand's interests internationally as well as protecting the State from security threats.[12]

11.13 GCSB is a signals intelligence agency. It specialises in the collection of information through electronic means. Its powers are therefore focused on intercepting

---

8 As we explain below, there is currently a gap in NZSIS's ability to assist Police, but this will be remedied by the New Zealand Intelligence and Security Bill 2016 (158-1).

9 Government Communications Security Bureau Act 2003, s 8A.

10 Section 8B.

11 Section 8C.

12 Section 7. The Act's stated objectives are to contribute to New Zealand's national security, the international relations and well-being of New Zealand and the economic well-being of New Zealand.

communications and accessing "information infrastructures" (which are broadly defined, including electromagnetic emissions as well as communications and information technology systems or networks[13]).

11.14 GCSB can obtain authorisation to intercept private communications or access information infrastructures where:[14]

- the interception or access is for the purpose of performing GCSB's cyber security or intelligence function;
- the outcome to be achieved justifies the interception or access;
- the outcome is not likely to be achieved by other means; and
- there are satisfactory arrangements in place to ensure the acts done in relation to the authorisation will be both reasonable and necessary for the proper performance of a GCSB function.

11.15 These grounds are broader than the criteria for issuing search warrants under the Search and Surveillance Act, in the sense that they do not require reasonable grounds to suspect specific offending or to believe evidential material will be found. Rather, the focus is on whether the activity is necessary for the purpose of performing the GCSB's functions and is proportionate to the outcome sought. The activity authorised under GCSB authorisations is also wider than that authorised under police warrants. A GCSB authorisation can apply to a class of persons, places or information infrastructures rather than identifying a specific target.[15]

### *NZSIS*

11.16 The main functions of NZSIS are to collect and evaluate intelligence relevant to security and provide advice on protective measures.[16] "Security" includes both internal and foreign threats to the State, such as espionage and terrorism.[17] NZSIS also has a vetting function in relation to people seeking security clearances and can make

---

13 Government Communications Security Bureau Act 2003, s 4 (definition of "information infrastructure").

14 Section 15A.

15 Section 15D. Although surveillance device warrants under the Act should generally identify a specific target, there is an exception provided where that is not possible in the circumstances (see ss 49(2) and 55(4)).

16 New Zealand Security Intelligence Service Act 1969, s 4.

17 Section 2 (definition of "security").

recommendations relevant to security in relation to the determination of citizenship and immigration matters.[18]

11.17 NZSIS is a human intelligence agency, which means it focuses on the use of human (as opposed to electronic) sources to obtain information. NZSIS can obtain "intelligence warrants" permitting it to intercept or seize communications, documents or things, or to undertake electronic tracking.[19] Intelligence warrants can authorise entry and search of the target premises and the installation and monitoring of equipment or devices.[20]

11.18 NZSIS warrants are currently required to be more specific than GCSB authorisations. They must identify the particular person, or if that is not possible, the place that is the subject of the warrant.[21] However, this would change under the New Zealand Security and Intelligence Bill. The Bill would allow warrants to authorise the carrying out of searches and surveillance activity for a specified purpose and reason rather than in respect of a specified person or place, where that is necessary to achieve the objective of the warrant.[22]

11.19 The criteria that must be satisfied before an intelligence warrant can be issued to NZSIS are similar to those applying to GCSB authorisations:[23]

- the interception, seizure or tracking must be necessary to detect activities prejudicial to security or to gather foreign intelligence essential to security;
- the value of the information sought must justify the proposed activity; and
- the information must be unlikely to be obtained by any other means.

## Comparison to police powers

11.20 The nature of the investigative activities or methods that police officers can carry out or use under the Search and Surveillance Act are similar to those permitted under the

---

18 New Zealand Security Intelligence Service Act 1969, s 4.

19 Section 4A(1)–(2).

20 Section 4E.

21 Section 4B.

22 New Zealand Intelligence and Security Bill 2016 (158-1), cl 64.

23 New Zealand Security Intelligence Service Act 1969, s 4A(3). In addition, any communications sought to be intercepted or seized must not be privileged. In the Government Communications Security Bureau Act 2003 this is dealt with by a separate section rather than as part of the warrant criteria (s 15C).

GCSB and NZSIS Acts. Warrants under the Act can authorise the use of interception, tracking and visual surveillance devices,[24] as well as entry, search and seizure.[25]

11.21 The key differences between the powers of Police and those of GCSB and NZSIS are the circumstances in which those activities can be authorised and how targeted they must be. For a police officer to obtain a search warrant or surveillance device warrant, they must establish that there are reasonable grounds:[26]

- to suspect that an offence specified in the application has been, is being or will be committed;[27] and
- to believe that the search or use of a surveillance device will obtain evidential material in respect of that offence.

11.22 These conditions mean that, unlike GCSB and NZSIS, police officers cannot generally use intrusive powers when they are simply gathering intelligence or undertaking the initial stages of investigating potential offending. police officers must use lawful techniques such as speaking to witnesses or receiving tips from informants to gain sufficient information to meet the "reasonable grounds" threshold for obtaining a warrant.

11.23 Unlike GCSB powers (but similar to NZSIS powers), the Act requires warrants to be as specific as possible. Search warrants must identify the particular place, vehicle or other thing that will be searched and must describe what may be seized.[28]

11.24 Surveillance device warrants by default are required to specify the person, place, vehicle or other thing that is the object of surveillance and the evidential material that may be obtained.[29] However, if this information cannot be provided, a warrant can instead state the "circumstances in which the surveillance is proposed to be undertaken in enough detail to identify the parameters of, and objectives to be achieved by, the

---

24 Search and Surveillance Act 2012, ss 3 (definition of "surveillance device") and 55.

25 Sections 6 and 55(3)(h).

26 Sections 6 and 51.

27 In general any imprisonable offence will qualify (ss 6 and 51(a)(i)). However, where a warrant is sought for the use of an interception device or trespassory use of a visual surveillance device, the offence must be punishable by at least seven years' imprisonment or be one of the other offences specified in the legislation (s 45).

28 Section 103(4)(f)–(g).

29 Section 55(3)(d)–(e).

proposed use of the surveillance device".[30] This provides a fair degree of flexibility, but still appears to require a greater degree of targeting than GCSB authorisations, which can apply to broad classes of people, places or information infrastructures.

## Current powers of GCSB and NZSIS to assist Police and other enforcement agencies

11.25 Neither GCSB nor NZSIS has a law enforcement function or a function of preventing and detecting crime. This means that they cannot generally use the powers available under their governing legislation to detect, prevent or investigate crime. However, there are two main ways in which they can contribute to these objectives.

### *Cooperating within the scope of intelligence and security functions*

11.26 GCSB and NZSIS sometimes collect intelligence that has links to crime or law enforcement in the course of performing their intelligence and security functions.

11.27 For example, NZSIS has a role in investigating and monitoring people who may be preparing to commit terrorist acts or espionage.[31] GCSB's foreign intelligence collection may relate to crimes by foreign persons that impact on New Zealand's interests, such as illegal fishing in New Zealand waters, money laundering or drug trafficking. GCSB may also come across information relating to cybercrime in the course of carrying out its cyber security function.[32]

11.28 Intelligence collected by GCSB or NZSIS can be provided to enforcement agencies where it is relevant to preventing or detecting crime punishable by two or more years' imprisonment.[33] So if, for example, NZSIS comes across information suggesting a crime has been or is about to be committed while it is carrying out its security intelligence functions, it can alert Police and provide them with the relevant information. Police can then conduct its own investigation into the offending where appropriate.

---

30 Search and Surveillance Act 2012, ss 49(2) and 55(4).

31 New Zealand Security Intelligence Service Act 1969, ss 2 (definition of "security") and 4(1)(a).

32 Government Communications Security Bureau Act 2003, s 8A.

33 Government Communications Security Bureau Act 2003, ss 4 (definition of "serious crime") and 25; New Zealand Security Intelligence Service Act 1969, s 4H.

11.29 Like any other government agency, GCSB and NZSIS can cooperate with other organisations to the extent that this falls within their functions.[34] For example, NZSIS and GCSB are both part of the Combined Threat Assessment Group, which carries out risk assessments relating to terrorist and criminal threats of physical harm to New Zealanders and New Zealand interests. The Group also includes Police, the New Zealand Defence Force, the New Zealand Customs Service and Maritime New Zealand.

11.30 We understand that, as a matter of practice, intelligence agencies may sometimes be reluctant to provide information to Police or other enforcement agencies due to discomfort about it being used as evidence in court. Intelligence information is often very sensitive, either because of the nature of the information itself or because of the capabilities or sources it might reveal. This is a practical rather than a legislative barrier, so we do not see it as a matter for this review.

### *Assisting in the performance of police functions*

11.31 GCSB also has a separate function of cooperating with, and providing advice and assistance to Police, the New Zealand Defence Force and NZSIS to facilitate the performance of those agencies' functions.[35] When performing this assistance function, GCSB must act within the scope of the other agencies' lawful functions and powers, and any restrictions or protections relating to them.[36] For example, if GCSB were to help Police intercept communications for the purpose of investigating a crime, it would do so under (and within the scope of) a surveillance device warrant issued to Police under the Search and Surveillance Act.

11.32 GCSB's assistance function was introduced in recognition of the high-end technological capability located within GCSB. While Police has its own capabilities to intercept communications and access information, these will not always be co-extensive with those of GCSB. Since technological capabilities are often costly to establish and maintain, it may not be efficient for Police to develop capabilities that they only need to access occasionally. The assistance function was intended to

---

34 See Government Communications Security Bureau Act 2003, s 8B(2).

35 Government Communications Security Bureau Act 2003, s 8C.

36 Section 8C.

circumvent the need to duplicate capability and assets across multiple government agencies.[37]

11.33 NZSIS does not currently have an equivalent function of assisting other agencies to perform their functions. It can cooperate with other agencies only to the extent practicable and necessary for the performance of its own functions.[38] However, under the New Zealand Intelligence and Security Bill, NZSIS would gain the same assistance function that GCSB has.[39]

### *Is there a gap in the current assistance regime?*

11.34 The current law allows intelligence agencies to cooperate with or assist enforcement agencies (in particular Police) to a relatively high degree. The main area we have identified where intelligence agencies cannot assist Police is when:

- their intelligence and security functions are not engaged (because the type of crime being investigated or monitored is not related to national security); *and*
- the assistance they wish to provide is outside the scope of police powers.

11.35 This is primarily likely to occur at the crime prevention or detection stage, where a warrant cannot be obtained (or a warrantless power cannot be exercised) under the Search and Surveillance Act because the relevant threshold (of reasonable belief) has not yet been established.

## APPROACHES IN OTHER JURISDICTIONS

11.36 Other jurisdictions generally allow some form of cooperation or assistance between intelligence agencies and Police, but the nature and extent of this differs. We summarise the approaches taken in Australia, Canada and the United Kingdom in the table below.

| ABILITY OF INTELLIGENCE AGENCIES TO ASSIST POLICE IN OTHER JURISDICTIONS | | |
|---|---|---|
| **Country** | **Intelligence agencies** | **Ability to assist Police** |
| **Australia** | Australian Signals | ASD and ASIS are generally prohibited from carrying out police |

[37] Intelligence Coordination Group *Departmental Report for the Intelligence and Security Committee*: *Government Communications Security Bureau and Related Legislation Amendment Bill* (July 2013) at [105]–[106].

[38] New Zealand Security Intelligence Service Act 1969, s 4(1)(c).

[39] New Zealand Intelligence and Security Bill 2016 (158-1), cl 16.

| | | |
|---|---|---|
| | Directorate (ASD)<br><br>Australian Secret Intelligence Service (ASIS)[40] | functions.[41] While they may assist a commonwealth or State authority prescribed by regulations,[42] which could include a law enforcement agency,[43] it appears that no such regulations have been made.<br><br>ASD and ASIS can:<br><br>• provide foreign intelligence to Police if it is relevant to serious crime;[44] and<br>• collect intelligence about an Australian person likely to be involved in specified transnational and signals-related crimes.[45] |
| | Australian Security Intelligence Organisation (ASIO)[46] | ASIO can cooperate with law enforcement agencies to help those agencies perform their functions.[47] In doing so ASIO is not expressly restricted to acting within the scope of police powers.<br><br>However, ASIO can only obtain warrants under its own legislation for security-related purposes.[48] In practice it would likely need to act under (and within the scope of) a police warrant if assisting in relation to non-security related crimes. |
| **Canada** | Communications Security Establishment (CSE)[49] | CSE can assist Police within the scope of police powers. |
| | Canadian Security Intelligence Service (CSIS)[50] | CSIS can only cooperate with Police for the purpose of performing its own functions (that is, where the cooperation is relevant to security).[51] |

40 The Australian Signals Directorate is Australia's signals intelligence agency (similar to GCSB in New Zealand). The Australian Secret Intelligence Service is a foreign human intelligence agency (this role is carried out to a limited extent by NZSIS alongside its domestic security intelligence function – there is no direct equivalent).

41 Intelligence Service Act 2001 (Cth), s 11.

42 Section 13A.

43 Section 11(2)(d)–(e).

44 Section 11(2)(c).

45 Section 9(1A).

46 The Australian Security Intelligence Organisation is a domestic security intelligence organisation (similar to NZSIS, except that NZSIS also has a limited foreign intelligence function).

47 Australian Security Intelligence Organisation Act 1979 (Cth), s 19A.

48 See for example Australian Security Intelligence Organisation Act 1979 (Cth), ss 25(2) (search warrants), 25A(2) (computer access warrants) and 26(3) (surveillance device warrants).

49 The Communications Security Establishment is Canada's signals intelligence agency (equivalent to GCSB in New Zealand).

50 The Canadian Security Intelligence Service is Canada's human intelligence agency (equivalent to NZSIS in New Zealand).

51 Canadian Security Intelligence Service Act RSC 1985 c C-23, s 17.

| | | |
|---|---|---|
| **United Kingdom** | Security Service<br><br>Secret Intelligence Service<br><br>Government Communications Headquarters | All of the United Kingdom intelligence agencies have an express function of supporting the prevention and detection of serious crime.[52] This means they can use their own powers for this purpose and are not restricted to using police powers.<br><br>In any case, surveillance powers for intelligence and law enforcement agencies are largely covered by the same legislation and subject to the same thresholds. For example, both Police and intelligence agencies can get an interception warrant if it is considered necessary for the purpose of preventing or detecting serious crime.[53] Police search warrants are, however, subject to a reasonable belief threshold.[54] |

11.37 The approaches in Canada and Australia are broadly similar to the New Zealand approach. Intelligence agencies can pass intelligence collected while performing their own functions to Police if it is relevant to crime (or certain types of crime). Some agencies also have the ability to assist Police to perform law enforcement functions, but must act within the scope of police powers.

11.38 The United Kingdom takes a more expansive approach. Intelligence agencies have an explicit role in preventing and detecting serious crime, so they may use any of the powers available under their legislation for that purpose.

## SHOULD GCSB AND NZSIS BE ABLE TO USE THEIR OWN POWERS FOR LAW ENFORCEMENT PURPOSES?

### Differences between intelligence gathering and law enforcement

11.39 The core role of Police is to enforce the law. Police investigations have traditionally focused on gathering evidence to prove specific instances of criminal offending, with the ultimate aim of bringing a prosecution.

11.40 In more recent decades law enforcement agencies across the globe have increased their focus on preventing crime as well. Crime prevention is recognised in statute as one of the functions of Police,[55] and the Search and Surveillance Act now allows Police to conduct search and surveillance activities on the basis of reasonable suspicion that an offence "will be committed" (earlier legislation required the offence to have already been committed). However, despite these moves toward a more preventative approach,

---

52 Intelligence Services Act 1994 (UK), ss 1(2) and 3(2); Security Service Act 1989 (UK), s 1(4).

53 Regulation of Investigatory Powers Act 2000 (UK), ss 5–6.

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

55 Policing Act 2008, s 9(d).

the Act still requires a close connection to a specific criminal offence before a search or surveillance power can be exercised.

11.41 By comparison, intelligence agencies collect and analyse a broad range of information about threats and opportunities in order to assist the government to make decisions that protect and advance the country's interests. This can cross over into areas where certain types of crimes are involved, such as espionage, terrorism and transnational crime. However, the purpose of intelligence operations is to monitor trends and inform policy decisions, not to investigate particular cases of criminal offending or to gather evidence to support a prosecution.

11.42 Criminal investigations may result in the State imposing punishment on individuals. The evidence obtained during an investigation may be used as a basis for arrest, prosecution and the deprivation of liberty. Because of this, the exercise of search and surveillance powers for law enforcement purposes has traditionally been subject to strict legal standards and, except in urgent circumstances, prior scrutiny by an independent judicial officer. This is necessary to maintain confidence in the justice system and to accord legitimacy to the use of coercive State power against individuals.

11.43 While intelligence gathering activity may be as intrusive as a criminal investigation, it is used for a different purpose: to inform policy or, in some cases, to prompt a full criminal investigation with the usual safeguards. Intelligence agencies do not have enforcement powers and intelligence information is rarely used as evidence in criminal proceedings.

### Changing the status quo would alter the nature of police investigations

11.44 As we have discussed above, the main difference between the powers of Police and intelligence agencies is not the type of capabilities or methods they are permitted to use, but rather the controls on the use of those methods. Intelligence agencies' powers can be exercised to proactively identify developing threats to New Zealand's interests or opportunities to advance those interests. They need not establish a link to suspected criminal offending in the same way that Police must and, in the case of GCSB, can carry out relatively broad foreign intelligence collection rather than targeting specific people or places.

11.45 We understand the main "gap" in the current legislation—where there may be scope for increased intelligence agency support for police functions—is in the crime prevention and detection area (as opposed to the investigation of specific offending).

In the same way that the intelligence agencies can exercise their powers to identify developing threats, there would be potential for them to use their capabilities (such as GCSB's relatively broad interception capability) to look for indications that crimes may be occurring or are being planned. In effect, that would amount to search or surveillance for law enforcement purposes but without meeting the threshold that Police and other enforcement agencies must meet under the Act.

11.46 We have identified two possible ways in which the law could be changed to allow this to occur. However, for reasons we explain below, our preliminary view is that neither of these changes is likely to be justified. The two possible changes are:

- The legislation governing GCSB and NZSIS could be amended to give those agencies an explicit function of contributing to the prevention and detection of crime (similar to the United Kingdom legislation). This would mean GCSB and NZSIS could use the powers they have under their own legislation for law enforcement purposes, without being constrained by the requirements in the Search and Surveillance Act.
- The Search and Surveillance Act could be amended to allow search and surveillance activities to be carried out before the point at which reasonable belief is established. This would involve lowering the current thresholds that must be met before exercising search and surveillance powers. These lower thresholds would apply to enforcement agencies, but also to GCSB and NZSIS when acting within the scope of police powers under their assistance function.

11.47 In relation to option (a), it seems undesirable to allow intelligence agencies to exercise their powers for law enforcement purposes in a broader way than Police can, given that law enforcement is primarily a police function. This would create an irrational distinction in the legislation and, as the Cullen/Reddy report recognised, would effectively expand police powers through a back door.[56]

11.48 Option (b) would, in essence, allow the use of search and surveillance powers for broader crime detection and monitoring purposes, without requiring a close connection to specific offending and the obtaining of evidential material. While there could be benefits to such an approach from a community safety perspective, it would

---

[56] Cullen and Reddy *Intelligence and Security in a Free Society*, above n 1, at [5.59].

fundamentally alter the balance between law enforcement and human rights values in a way that we do not think the New Zealand public would support.

11.49 As we have noted in Chapter 3, expanding search and surveillance activity for law enforcement purposes beyond the investigation of specific offences could be seen as treating the general public as suspects. It is likely to have a chilling effect on the exercise of rights such as freedom of expression. Arguably, it is incompatible with the values underpinning free and democratic societies.

11.50 While national security has long been recognised as an area where some intrusive monitoring or detection activities are required, strong justification would be needed to extend equivalent powers to a law enforcement context. So far we have seen nothing to convince us that such justification exists.

Q49 Is there any justification for allowing intelligence agencies' capabilities to be used for law enforcement purposes beyond the current scope of police powers?

# Appendix A

## TERMS OF REFERENCE FOR THE STATUTORY REVIEW OF THE SEARCH AND SURVEILLANCE ACT 2012

Section 357 of the Search and Surveillance Act 2012 (the Act) requires the Minister of Justice to refer a review of the operation of the Act to the Law Commission and the Ministry of Justice by 30 June 2016. The Law Commission and the Ministry of Justice must report jointly to the Minister of Justice within one year of that referral.

The terms of reference for the review are as follows.

1. As required by s 357 of the Act, the review will consider:
    - the operation of the provisions of the Act since 1 October 2012;
    - whether they should be retained or repealed; and
    - whether any amendments to the Act are necessary or desirable.
2. The review will identify and focus on core policy issues. Smaller or more technical matters will be worked through by the Ministry of Justice with the intention that they be implemented at the same time as any reforms made as a consequence of the review.
3. Without limiting the scope of the review, the Law Commission and the Ministry of Justice will consider whether any changes to the Act are required to ensure it enables effective law enforcement and maintains consistency with human rights laws, now and into the future, in light of:
    - developments in technology and their broader implications;
    - any significant case law on, or relevant to the review of, the Act since its enactment; and
    - international legislative developments relating to search and surveillance since the Act's enactment.
4. As suggested in the report of the First Independent Review of Intelligence and Security, the review will also consider whether the Act (or any related legislation) should be amended to enable broader use of the capabilities of the Government Communications Security Bureau and/or New Zealand Security Intelligence Service to support police investigations.

5. The process for the review will include:

- inviting public submissions;
- consultation with relevant government agencies and private sector organisations; and
- establishing an expert advisory panel to provide technical expertise and advice representing a range of perspectives.

# Appendix B

## EXCERPT FROM A TEMPLATE FOR A SEARCH WARRANT

Section 103(4)(l) of the Search and Surveillance Act 2012 requires every search warrant to contain an explanation of the availability of relevant privileges and an outline of how those privileges may be claimed (where applicable). The following excerpt is an example of that explanation, taken from a template supplied to us by New Zealand Police:

> **Rights to bring claim of privilege**
>
> The owner of any thing seized or the person from whom it is seized has the right to bring a claim to have the thing recognised as subject to one of the following privileges:
>
> (a) legal professional privilege to the extent (under section 53(5) of the Evidence Act 2006) it forms part of the general law;
>
> (b) privilege for communication with legal advisers;
>
> (c) privilege for preparatory material to proceedings;
>
> (d) privilege for settlement negotiations or mediation;
>
> (e) privilege for communication with ministers of religion;
>
> (f) privilege in criminal proceedings for information obtained by medical practitioners and clinical psychologists;
>
> (g) privilege for informers;
>
> (h) the rights conferred on a journalist under section 68 of the Evidence Act 2006 to protect certain sources.
>
> If you need any further information about the nature of these rights and privileges, or whether they may apply to any items that have been or may be seized, you are advised to seek legal advice.
>
> Any person who wishes to claim privilege in respect of any thing seized or sought to be seized by the police officer in charge of executing a search warrant or exercising a search power:
>
> (a) must provide the police officer in charge of undertaking the search with a particularised list of the things in respect of which the privilege is claimed, as soon as practicable after being provided with the opportunity to claim privilege or being advised that a search is to be, or is being, or has been conducted; and
>
> (b) if the thing or things in respect of which the privilege is claimed cannot be adequately particularised in accordance with paragraph (a), may apply to a District Court for directions or relief (with a copy of the thing provided under section 146(b) of the Search and Surveillance Act).

# Appendix C

## GLOSSARY

| GLOSSARY OF FREQUENTLY USED TERMS | |
|---|---|
| **amicus curiae** | A person appointed by a court to provide impartial advice on an aspect of the law or to advance legal arguments on behalf of a party who is not represented by legal counsel. |
| **Closed-Circuit Television (CCTV)** | A self-contained surveillance system comprising cameras, recorders and displays for monitoring activities in public or on private premises. |
| **cloud computing** | Storing and accessing data and programs using remote servers hosted on the Internet, rather than on a local server or personal computer. |
| **computer system** | Defined in section 3 of the Search and Surveillance Act 2012 as a computer; or two or more interconnected computers; or any communication links between computers or to remote terminals or another device; or two or more interconnected computers combined with any communication links between computers or to remote terminals or any other device. This includes any part of the items described and all related input, output, processing, storage, software, or communication facilities, and stored data. |
| **curtilage** | The land immediately surrounding a house or building, including any closely associated buildings and structures, but excluding any associated open fields beyond them. The term is not defined in the Act. |
| **digital forensics unit (DFU)** | A discrete unit within an enforcement agency that is responsible for conducting digital searches. |
| **electronic devices** | All devices that operate with components such as microchips and transistors that control and direct electric currents. This includes but is not limited to computers, tablets and mobile phones. |
| **encryption** | The process of converting information such as a text or email message into an encoded format that can only be decrypted and read by someone with access to a secret key. |
| **enforcement officer** | Defined in section 3 of the Act as a constable; or any person authorised by an enactment specified in column 2 of the Act's Schedule, or by any other enactment that expressly applies any provision in Part 4, to exercise a power of entry, search, inspection, examination, or seizure. |
| **enforcement agency** | Defined in section 3 of the Act as any department of State, Crown entity, local authority, or other body that employs or engages enforcement officers as part of its functions. |
| **flight mode** | A setting on a mobile phone or wireless gadget that disables the device's signal-transmitting ability but allows for the use of its other functions. The setting is typically engaged for safe use on an airplane where activities that require signal transmission are forbidden. |

| | |
|---|---|
| **forensic image** | A forensically sound and complete copy of a hard drive or other digital media, including deleted and hidden data. |
| **Global Positioning System (GPS)** | A satellite navigation system used to determine the ground position of an object. |
| **information infrastructure** | Defined in section 4 of the Government Communications Security Bureau Act 2003 as including electromagnetic emissions, communications systems and networks, information technology systems and networks, and any communications carried on, contained in, or relating to those emissions, systems, or networks. |
| **International Mobile Subscriber Identity (IMSI)** | A number located in a mobile phone's subscriber identification module (SIM) card, which identifies the subscriber. |
| **Internet Protocol (IP) address** | A unique address that identifies a device on the Internet or a local network. |
| **internet service provider (ISP)** | An organisation that provides services for accessing and using the Internet. |
| **issuing officer** | Defined in section 3 of the Search and Surveillance Act 2012 as a District Court or High Court judge; or a person such as a Justice of the Peace, Community Magistrate, Registrar, or Deputy Registrar, who is for the time being authorised to act as an issuing officer under section 108 of the Act. |
| **keystroke logging** | The use of a software program to monitor keystrokes that a user types on a computer's keyboard. |
| **local area network (LAN)** | A computer network limited to a small area such as an office building, university, or even a residential home. |
| **metadata** | Data about data. It includes data created when forms of electronic communication are made – for example, 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 and received from. It does not include the content of communications, such as the body of an email. |
| **optical character recognition (OCR)** | The mechanical or electronic conversion of images of typed, handwritten or printed text into machine-encoded text. |
| **remote access search** | Defined in section 3 of the Act as a search of a thing such as an Internet data storage facility that does not have a physical address that a person can enter and search. |