



REVIEW OF THE SEARCH AND SURVEILLANCE ACT 2012

KO TE AROTAKE I TE SEARCH AND SURVEILLANCE ACT 2012

Law Commission / Te Aka Matua o te Ture

The Law Commission / Te Aka Matua o te Ture is an independent, publicly funded, central advisory body established by statute to undertake the systematic review, reform and development of the law of New Zealand. Its purpose is to help achieve law that is just, principled and accessible, and that reflects the heritage and aspirations of the peoples of New Zealand.

The Commissioners are the Hon Douglas White QC (President), Donna Buckingham, Helen McQueen, and Hon Dr Wayne Mapp QSO. The General Manager is Jasmine Tietjens.

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
Email: com@lawcom.govt.nz
Internet: www.lawcom.govt.nz

Ministry of Justice / Tāhū o te Ture

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: www.justice.govt.nz

The Māori language version of the Report's title was developed for the Commission and the Ministry by Kiwa Hammond, Tohuao and Toi Reo Māori.

Cover image by Thomas Kvistholt on Unsplash (<https://unsplash.com/photos/oZPwn40zCK4>).

A catalogue record for this title is available from the National Library of New Zealand. Kei te pātengi raraunga o Te Puna Mātauranga o Aotearoa te whakarārangi o tēnei pukapuka.

ISBN: 978-1-877569-81-4 (Print)
ISBN: 978-1-877569-80-7 (Online)

ISSN: 0113-2334 (Print)
ISSN: 1177-6196 (Online)

This title may be cited as NZLC R141

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

27 June 2017

Hon Mark Mitchell
Associate Minister of Justice
Parliament Buildings
WELLINGTON

Dear Minister

NZLC R141 – Review of the Search and Surveillance Act 2012
Ko te Arotake i te Search and Surveillance Act 2012

We are pleased to submit to you the above Report under section 357 of the Search and Surveillance Act 2012.

Yours sincerely



Douglas White
President
Law Commission / Te Aka Matua o te Ture



Rajesh Chhana
Deputy Secretary Policy
Ministry of Justice / Tāhū o te Ture

Foreword

Legislation frequently does not tell enforcement officers what coercive powers they have or how they are to exercise them. Far too much is therefore left to their individual discretion and judgement. Courts are left to determine the legality and reasonableness of their actions after the event, usually in the context of challenges to the admissibility of evidence in subsequent criminal proceedings. This unnecessarily occupies valuable court time in resolving the disputes that inevitably arise. In a liberal democratic society ... the exercise of coercive powers by the state should be subject to clear and principled controls ...

Sir Geoffrey Palmer

These words appear in the foreword to the Law Commission's 2007 Report, *Search and Surveillance Powers*. It was the most substantial report that the Commission had then produced, making 300 recommendations on the use of investigative and evidence-gathering powers by law enforcement agencies.

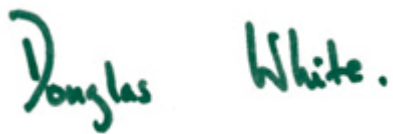
The Search and Surveillance Act 2012 ultimately responded to the challenge of bringing coherence, clarity and consistency to this area of the law. It went further than the scope of the Commission's original review, which had focused on criminal law enforcement. Some of the Act's provisions also extend to those who ensure compliance with regimes that regulate many lawful activities.

Yet the foreword comment in the Commission's original Report still provides the underlying theme of this review of the Act, which has been jointly conducted by the Law Commission and the Ministry of Justice over the course of one year. The review itself and its timeframe were mandated by the Act, in recognition of the significant changes its provisions made to search and surveillance law.

The terms of reference require this review to reflect the relationship between the two public interests lying at the heart of the Act. The first is the need to equip enforcement agencies effectively and adequately for their role in protecting the public by detecting and prosecuting offending or by enforcing regulatory compliance; the second is the need to ensure that this role is clearly regulated, able to be audited and only occurs where it is justified. In other words, law enforcement must only intrude on the protection of individuals' rights to privacy, dignity and property to the extent that the intrusion is necessary and proportionate.

Five years on from the Act's commencement, rapid changes in both technology and in the way crimes are committed have altered the context in which the Act must operate. This review assesses how the Act's provisions are working and does so against the background of that technological change and in the light of significant case law and international legislative developments.

That has required consideration of how the Act can balance the public interests in effective law enforcement and in the protection of human rights values in this new environment and how to ensure, as far as possible, that it will continue to do so in the future.



Douglas White
President
Law Commission / Te Aka Matua o te Ture



Rajesh Chhana
Deputy Secretary Policy
Ministry of Justice / Tāhū o te Ture

Acknowledgements

We gratefully acknowledge all those who helped us to isolate issues with the current legislation or who provided a submission or comment on those issues or a view on the proposals we formulated. This includes members of the judiciary, representatives from enforcement agencies, the legal profession, other institutions or organisations and members of the public. A list appears in Appendix 3.

Members of our Expert Advisory Group were chosen for their wide variety of technical or legal expertise in privacy and human rights, investigative and surveillance technology, trial process and evidential issues. While the recommendations in this Report remain those of the Commission and the Ministry, the group's collective wisdom was very valuable in consolidating or amending our thinking around those proposals. The members of the Advisory Group were:

- Dr Andrew Butler
- Nick Chisnall
- Katrine Evans
- Dr David Harvey
- Maarten Kleintjes
- Associate Professor Scott Optican
- Dean Pemberton

Our Officials Group included representatives from the New Zealand Police, Department of Internal Affairs, Inland Revenue, Crown Law Office, Department of the Prime Minister and Cabinet, Ministry for Primary Industries, New Zealand Customs Service and Ministry of Business, Innovation and Employment. The group provided helpful guidance on the issues we selected for our Issues Paper and also engaged in rigorous discussion of our preliminary policy proposals.

The Commissioner responsible for this reference was Donna Buckingham. The legal and policy advisers for this Report were Dena Valente (Ministry of Justice), Kate Salmond (Law Commission), Yasmin Moinfar-Yong (Law Commission), Linda McIver (Law Commission) and Hanna Shaw (Ministry of Justice). The assisting Commission law clerks were Emily Watson, Rebecca McMenamin and Fady Girgis.

Contents

Foreword	iv
Acknowledgements	vi
Executive summary	6
The scope of the review	6
The objectives of the review	7
Overview of the Act	8
What is wrong with the current law?	9
Overview of the reforms	11
Areas where we do not recommend reform	15
Further work to be undertaken	15
List of recommendations	16
PART 1 Overarching issues	33
Chapter 1 Introduction	34
Origins of the Search and Surveillance Act 2012	34
The statutory requirement to conduct a review	35
The review process	35
The structure of this Report	36
Future reviews of the Act	37
Chapter 2 Underlying themes	38
Introduction	38
Values underpinning the Act	38
Privacy	39
Effectiveness	49
Section 30 of the Evidence Act 2006	54
Law enforcement and regulatory powers	55
The concept of informed consent	58
Chapter 3 The case for a principles provision	60
Introduction	60
The value and functions of principles provisions	60
The case for a principles provision in the Act	62
The principles provision	64
Chapter 4 The principles	68
Introduction	68
Preliminary issues	68

Principle 1: using statutory mechanisms to carry out intrusive activity	69
Principle 2: warrant preference	74
Principle 3: proportionality	77
Principle 4: minimising privacy intrusions	81
Principle 5: te ao Māori and cultural, spiritual or religious considerations	83
Principle 6: minimising impact on children and vulnerable people	87
Principle 7: privilege	87
Chapter 5 Policy statements	91
Introduction	91
Background	91
Purpose of policy statements	93
Effect of policy statements	93
Activity that should be covered by policy statements	94
Process for issuing policy statements	95
Chapter 6 Declaratory orders	99
Introduction	99
Background	99
Consultation	102
The case against residual warrants	103
Retaining the declaratory order regime	104
Clarifying the declaratory order regime	111
PART 2 Surveillance	115
Chapter 7 Scope of surveillance powers	116
Introduction	116
Overview of the surveillance device regime	116
Surveillance not covered by the regime	118
Surveillance for non-evidential purposes	128
Chapter 8 Availability of surveillance powers	132
Introduction	132
Background	132
Offence threshold	133
Who can apply for surveillance warrants	140
Who can issue surveillance warrants	145
Chapter 9 Interception and tracking	146
Introduction	146
Scope of the interception warrant requirement	146
Interception with consent	150
Incidental interception	154
Exceptions to the tracking warrant requirement	156

Relationship between tracking and other surveillance	159
Chapter 10 Surveillance: procedural matters	161
Introduction	161
Entry to third-party premises	161
Removal of surveillance devices	164
Retention of raw surveillance data	166
Chapter 11 Public surveillance	169
Introduction	169
The current legal framework	170
Public surveillance and expectations of privacy	172
Consultation	174
Policy statements for public surveillance	175
Public surveillance not covered by policy statements	184
PART 3 Search	187
Chapter 12 Digital searches	188
Introduction	188
Terminology	188
Structure and summary of recommendations	189
Overview of the provisions in the Act	192
The nature of electronic devices	192
A warrant requirement	194
The content of the warrant	197
Issues raised by Internet searches	202
The Internet search provisions in the Act	210
Access information	220
Chapter 13 Warrantless powers	226
Introduction	226
Current law	227
Thresholds for exercising warrantless powers	227
Tampering with electronic monitoring devices	229
Chapter 14 Production orders	233
Introduction	233
The production order regime in the Act	234
Production powers in other legislation	237
Disclosure of documents under the Privacy Act 1993	239
A statutory requirement to obtain a production order	242
A production order policy statement	246
The financial cost of production orders	250
Notification	251

Reporting	256
A data preservation regime	259
Extraterritorial production orders	264
PART 4 Other investigatory methods	267
Chapter 15 Covert operations	268
Introduction	268
The nature of covert operations	269
The current legal framework in New Zealand	271
Recent Supreme Court decisions	277
Consultation	280
The case for regulating covert operations	282
Overview of our proposed covert operations regime	286
Covert operations warrants	287
Policy statements	296
External audits	297
Immunities	299
Assumed identity information	300
Chapter 16 Examination orders	302
Introduction	302
Background	302
Consultation	304
Why the examination order regime should be retained	305
PART 5 Other matters	307
Chapter 17 Privilege	308
Introduction	308
Background	308
The privilege against self-incrimination and production orders	310
Providing information about privilege with production and examination orders	311
Out-of-court resolution of privilege claims	312
Chapter 18 Assistance from intelligence agencies	315
Introduction	315
Background	315
Consultation	315
Our view	317
APPENDICES	319
Appendix 1 Terms of reference	320
Appendix 2 Glossary	321

Appendix 3 List of submitters and consultees	324
Makers of submissions or comments	324
Consultation list	325

Executive summary

THE SCOPE OF THE REVIEW

- 1 This Report is the product of a unique joint review of the Search and Surveillance Act 2012 (the Act) conducted by the Law Commission and the Ministry of Justice. As required by the Act, it has been completed within one year of receiving the terms of reference.¹
- 2 The terms of reference asked the Commission and Ministry to consider the operation of the provisions in the Act since 1 October 2012 and to determine whether any amendments are necessary or desirable. Our objective is to ensure that the Act enables effective law enforcement and maintains consistency with human rights laws, now and into the future, in light of developments in:
 - technology;
 - case law; and
 - international search and surveillance legislation.
- 3 The terms of reference directed us to focus on core policy issues, so we have not conducted a systematic review of every provision. The Act has 357 sections. It contains the investigative powers of entry, search, seizure and surveillance that are available to New Zealand Police (and in some cases to other enforcement agencies) and provides detailed rules as to how they should be exercised.² Given the size and breadth of the Act, we had to be selective in deciding what issues to address.
- 4 During the initial research and consultation phase we became aware of an array of potential issues with the operation of the Act. We chose to focus on the most significant issues that would benefit from public consultation. In November 2016, we published our Issues Paper, *Review of the Search and Surveillance Act 2012*, which canvassed those issues.³ We deal with the same issues in this Report. We recorded problems with the Act of a more technical nature in a register. As our terms of reference indicate, the intention is that these will be worked through by the Ministry of Justice as part of any work to implement reforms made as a consequence of this review.
- 5 A specific question about whether the capabilities of New Zealand’s intelligence agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS)) should be used for law enforcement purposes to a greater extent than they are now was also included in the terms of reference. We address that question in Chapter 18 of this Report.

1 We note that, as we indicate in a number of areas in this Report, further work will be required by the Ministry of Justice before any amendments are made to the Search and Surveillance Act 2012 as a result of this review.

2 “Enforcement agency” is defined in s 3 of the Search and Surveillance Act 2012 as any department of State, Crown entity, local authority, or other body that employs or engages enforcement officers as part of its functions. An “enforcement officer” is 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. See also paragraphs [16]–[18] below and Chapter 2 at paragraphs [2.75]–[2.85].

3 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016).

- 6 We do not otherwise discuss the intelligence collection powers of GCSB and NZSIS in this Report because their powers are contained in the Intelligence and Security Act 2017, not the Search and Surveillance Act. Those agencies are tasked with contributing to the protection of New Zealand’s national security (including against terrorist threats), international relations and economic wellbeing.⁴ Their objectives do not include law enforcement, which the Search and Surveillance Act is concerned with.⁵
- 7 This Report also does not discuss the issue of whether the general search warrant regime is an appropriate mechanism for seizing a bodily sample (a question raised but not determined in *T v R*).⁶ The Law Commission is conducting a separate reference on the use of DNA in criminal investigations, which will consider that issue.⁷

THE OBJECTIVES OF THE REVIEW

- 8 The purpose of the Search and Surveillance 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”.⁸ This purpose reflects the two sets of values that arise in the context of regulating search and surveillance powers: human rights values and law enforcement values.
- 9 In its 2007 Report, *Search and Surveillance Powers* (which led to the enactment of the Search and Surveillance Act), the Law Commission explored these two sets of values in considerable detail.⁹ The Commission considered the principal human rights values engaged by search and surveillance powers were:¹⁰
- the protection of privacy;
 - the protection of personal integrity;
 - the protection of property rights; and
 - the maintenance of the rule of law.
- 10 The Commission considered the relevant law enforcement values at stake were:¹¹
- effectiveness;
 - simplicity;
 - certainty;
 - responsiveness to different types of operational circumstances; and
 - framing search powers in a manner that is human rights consistent.
- 11 Over the last ten years, developments in technology appear to have heightened the public’s interest in the privacy of their information and have created new opportunities and challenges

4 Intelligence and Security Act 2017, ss 9 and 58.

5 Section 13 of the Intelligence and Security Act states that co-operation with Police is a function of the intelligence agencies but that it must be performed subject to the same constraints that are placed on Police.

6 In *T v R* [2015] NZHC 1588 and *T v R* [2016] NZCA 148, the High Court and Court of Appeal observed that there is doubt as to whether the power to issue a search warrant in respect of a “thing” in s 6 of the Search and Surveillance Act 2012 can be interpreted to enable a search of human tissue.

7 That reference commenced on 27 July 2016 and involves a review of the Criminal Investigations (Bodily Samples) Act 1995.

8 Search and Surveillance Act 2012, s 5.

9 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) ch 2.

10 At [2.11].

11 At [2.26].

for effective law enforcement.¹² We have focused on privacy and effective law enforcement throughout this Report.

- 12 Significantly, in its original 2007 Report, the Commission did not see law enforcement values and human rights values as necessarily competing with one another.¹³ With this in mind, we have formulated our recommendations in this Report with a view to recognising both human rights values and law enforcement values to the greatest extent possible. On occasion, however, compelling reasons exist for one value to take precedence over the other. Where that is the case we have sought to acknowledge this and explain why we reached that conclusion.

OVERVIEW OF THE ACT

- 13 The Act contains five Parts. Part 1 contains general provisions and Part 5 contains amendments, repeals and miscellaneous provisions. Parts 2, 3 and 4 are the focus of our Report.

Parts 2 and 3

- 14 Parts 2 and 3 of the Act contain various search and surveillance powers that enable Police and other enforcement agencies to gather information to assist in the investigation and prosecution of offences and monitoring of compliance with the law. Some of these powers may also be used to prevent offending.¹⁴

- 15 Most of the powers in Part 2 of the Act are warrantless search powers. These can only be exercised by police constables. Other powers in Parts 2 and 3 require pre-authorisation in the form of a warrant or order issued by an independent issuing officer.¹⁵ The following warrants and orders are available:

- (a) **Search warrant** – a search warrant empowers an enforcement officer¹⁶ to search a specified place, vehicle or thing. Only constables can apply for a search warrant under the Act (although some other enforcement officers have the ability to apply for search warrants under other legislation).
- (b) **Examination order** – an examination order requires the person named in the order to attend at a specified time and place and to answer questions put to them by the Commissioner of Police (or their delegate). Only police officers of inspector rank or higher can apply for an examination order and only in limited circumstances.
- (c) **Surveillance device warrant** – a surveillance device warrant empowers an enforcement officer to use an interception, tracking or visual surveillance device. Where warrants would authorise visual surveillance involving trespass or interception, they can only be applied for by constables and a higher threshold must be met.
- (d) **Production order** – a production order requires a person who is in possession of specified documents to hand those documents over to an enforcement officer.

12 This is discussed further in Chapter 2 at paragraphs [2.34]–[2.42].

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

14 The prevention of offending is not referred to in the purpose provision as an objective of the Act. However, some of the powers in the Act may be exercised for this purpose. For example, a warrantless power of entry may be exercised to prevent an offence or avert an emergency (s 14). Similarly, some of the recommendations in our Report relate to law enforcement activities that may be directed primarily towards offence prevention, for example, the recommendations in Chapter 11 concerning public surveillance.

15 An issuing officer is defined in s 3 of the Act as meaning a judge or a person such as a Justice of the Peace, Community Magistrate, Registrar, or Deputy Registrar, who is authorised to act as an issuing officer under s 108 of the Act.

16 An enforcement officer is defined in s 3 of the Act as meaning a constable or any person authorised by an enactment specified in column 2 of the Schedule, or by any enactment that expressly applies any provision in Part 4, to exercise a power of entry search, inspection, examination or seizure. We identify various officials who are enforcement officers under the Act in paragraph [18].

- (e) **Declaratory order** – a declaratory order is a statement by a judge that the use of a specified investigative technique is lawful and reasonable in the particular circumstances of the case.

Part 4

- 16 Part 4 of the Act sets out general provisions in relation to the exercise of search, surveillance and inspection powers by any enforcement officer. 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.
- 17 The extent to which Part 4 applies to the exercise of a power by any non-Police enforcement officers is set out in the Schedule of the Act. The Schedule lists the powers in other legislation that all or part of Part 4 applies to and the specific provisions in Part 4 that apply. The Schedule refers to 78 other statutes.
- 18 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, customs officers, investigators at Inland Revenue and the Department of Internal Affairs, animal welfare inspectors, fisheries inspectors, product safety officers, gambling inspectors, immigration officers, park rangers and wildlife rangers.

WHAT IS WRONG WITH THE CURRENT LAW?

- 19 Our view is that the Search and Surveillance Act is generally working well. None of our recommendations propose a major overhaul of the Act. We consider that some areas of the Act would benefit from clarification and that, in other areas, it is worth updating the Act to reflect international trends in search and surveillance law. We have also identified two wider problems:
- key aspects of search and surveillance law are contained in case law and are not evident on the face of the Act; and
 - the Act has not kept pace with developments in technology.

Key aspects of case law are not reflected in the Act

- 20 The Act was designed to clarify, rationalise and (to the extent possible) codify the law relating to the search and surveillance powers of law enforcement agencies. (The Act did not attempt to codify the powers of regulatory agencies, which are partially located in other legislation.¹⁷) However, key aspects of the law relating to search and surveillance remain in case law. This is not in keeping with the law enforcement values of simplicity and certainty, or with the rule of law, which requires the law to be accessible.
- 21 The problem stems from the way the Act is structured. In relation to some investigative activities, the Act is silent. In relation to other investigative activities, the Act empowers enforcement officers and issuing officers to make various decisions but does not always spell out the factors the officers need to take into account. These gaps are then filled by case law.
- 22 By way of example, the Act takes a permissive approach to search warrants. The Act empowers an enforcement officer to apply for a search warrant and gives an issuing officer the discretion to issue a search warrant if the statutory criteria are met. The Act does not require a search warrant to be obtained or issued in any given circumstances. In order to make decisions about

17 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [62]–[64].

the appropriate course of action in a case, enforcement and issuing officers must consider a range of factors that are not contained in the Act. Instead, they are identified in the case law surrounding section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA).

- 23 Section 21 of NZBORA protects individuals from “unreasonable search or seizure”. The case law stemming from this provision explains that a “search” is activity that amounts to a State intrusion upon a person’s reasonable expectation of privacy.¹⁸ This can include surveillance and requiring a person to produce documents. The case law also provides guidance on when a search is “lawful” and “reasonable”. Evidence obtained as a result of an unlawful or unreasonable search is “improperly obtained” for the purposes of the Evidence Act 2006 and may be ruled inadmissible at trial.
- 24 The jurisprudence arising from section 21 of NZBORA and section 30 of the Evidence Act is crucial to the operation of the Search and Surveillance Act. It explains when an enforcement officer should obtain a warrant or order and how search powers should be executed. However, its existence and relevance is not evident on the face of the Act. As we explain further below, we think that there are steps that can be taken to make the guidance in the case law more prominent, whilst retaining sufficient flexibility to respond to operational needs. This would ensure that relevant factors are addressed in each case in advance of a search occurring, rather than being considered in hindsight during any “back-end” section 30 admissibility inquiry.¹⁹

The Act has not kept pace with developments in technology

- 25 The Search and Surveillance Act reflects many of the recommendations that the Law Commission formulated in its 2007 Report, *Search and Surveillance Powers*. Work on that Report began in 2001. The way in which offences are committed and investigated has changed markedly since the Act came into force, and even more so over the last 16 years. The developments in technology of particular note are:
- the volume and diversity of data stored in electronic form has grown exponentially;
 - increasingly sophisticated electronic devices²⁰ have become ubiquitous;
 - there has been a rise in the use of cloud computing;²¹
 - it has become easier to hide electronic data using encryption and anonymisation tools;²² and
 - new surveillance technologies have become readily available.
- 26 These developments have created both opportunities and challenges for law enforcement and regulatory compliance. In terms of opportunities, there is more electronic evidence than ever before. As a society we now routinely generate copious amounts of data that can be used to re-create the actions, and even the intentions, of individuals. Text messages, emails, posts on

18 See *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [163] per Blanchard J, together with *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22].

19 We note that our review has not been concerned with the operation of s 30 of the Evidence Act 2006 itself. That section is specifically being considered by the Law Commission in the context of its second statutory review of the Evidence Act, which commenced in February 2017. The Law Commission must report to the Minister of Justice by 20 February 2019.

20 An “electronic device” is any device that is capable of storing data. This includes computers, mobile phones, tablets, digital cameras, hard drives, USB sticks and memory cards.

21 Cloud computing involves storing and accessing data and programs using remote servers hosted on the Internet, rather than on a local server or personal computer.

22 Encryption is 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.

social media,²³ CCTV footage,²⁴ bank statements and online travel bookings can all be used in this way. Further, new surveillance technology has developed that allows for the activities of individuals to be monitored in real time. However, to capitalise on these opportunities, the Act would need to provide clearer rules for accessing stored data or for utilising new surveillance techniques. Those rules would need to promote effective law enforcement and accommodate legitimate privacy concerns.

- 27 In terms of the challenges posed by technology, the rise in the use of cloud computing, encryption and anonymisation has made it increasingly difficult for enforcement agencies to locate and gain access to relevant data. We think that the Act could do more to provide enforcement agencies with the tools that are necessary to combat these challenges.

OVERVIEW OF THE REFORMS

- 28 The most significant recommendations in our Report are outlined below. These recommendations reflect either a change in policy since the enactment of the Act or a new policy. We also briefly summarise our recommendations that relate to procedural matters and/or aim to clarify existing law.

Principles

- 29 One of our main recommendations is that the Act should contain a principles provision.²⁵ This reflects our view that too much of the law in this area is contained in the jurisprudence surrounding section 21 of NZBORA.
- 30 The principles we propose are primarily based on existing case law and would inform decisions as to when and how search powers are exercised under the Act. Our goal is to promote greater clarity and transparency in relation to these decision-making processes, which will enhance effective law enforcement.
- 31 We recommend that the Act should provide for enforcement officers and issuing officers to take into account the following principles:
- conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement;²⁶
 - a warrant or order should be obtained in preference to exercising a warrantless power;²⁷
 - State intrusion into an individual's privacy should be proportionate to the public interest in the investigation and prosecution of the offence or the maintenance of the law;²⁸

23 "Social media" refers to internet-based communication platforms that enable users to share information (including messages, videos, pictures and any other content). Examples include Facebook, Twitter, Instagram, Snapchat, web forums and blogs.

24 Closed-Circuit Television (CCTV) is a self-contained surveillance system comprising cameras, recorders and displays for monitoring activities in public or on private premises.

25 The case for a principles provision is set out in Chapter 3. Chapter 4 discusses the principles that we recommend should be included in that provision.

26 Chapter 4 at paragraphs [4.6]–[4.27]. We discuss policy statements generally and make recommendations in respect of the statutory framework governing policy statements in Chapter 5.

27 Chapter 4 at paragraphs [4.28]–[4.43].

28 Chapter 4 at paragraphs [4.44]–[4.56].

- powers under the Act should be exercised:
 - in a manner that minimises the level of intrusion on the privacy of any individual likely to be affected;²⁹
 - having regard to te ao Māori (the Māori dimension) and any other relevant cultural, spiritual or religious considerations;³⁰
 - in a manner that minimises the impact on children and vulnerable members of the community;³¹ and
 - in a manner that protects any privilege held by, or available to, any individual.³²

32 We decided against including a stand-alone principle that explicitly recognises law enforcement values.³³ Effective law enforcement is fundamental to the Act, as recognised in the purpose provision. However, the importance of those values is already reflected in the provisions in Parts 2 and 3 of the Act that empower enforcement agencies to conduct various types of search and surveillance activity.

Policy statements

33 Where an investigative activity is lawful, there may still be doubt as to the reasonableness of undertaking the activity in any particular case. If a search is conducted unreasonably, it will breach section 21 of NZBORA. Again, the case law surrounding this provision is crucial.

34 To increase certainty and to promote transparency and accountability, we recommend that the chief executives of enforcement agencies should be required to issue publicly available policy statements in relation to certain investigative activities. These policy statements would be similar to the guidance relating to strip searches that Police is already required to publish under the Act.³⁴

35 We recommend that policy statements should be published in relation to public visual surveillance (including the use of CCTV cameras), social media monitoring, directed surveillance,³⁵ conducting interception or tracking surveillance with consent,³⁶ covert operations³⁷ (which we discuss further below) and production orders.

36 The production order policy statement is slightly different to the other policy statements we recommend, as the Act already regulates production orders. However, there are several ways in which enforcement officers can obtain documentary evidence, and there is doubt as to when it is appropriate to obtain a production order.³⁸ In those circumstances, a policy statement would provide valuable guidance for officials and the public at large.

29 Chapter 4 at paragraphs [4.57]–[4.68].

30 Chapter 4 at paragraphs [4.69]–[4.84].

31 Chapter 4 at paragraphs [4.85]–[4.88].

32 Chapter 4 at paragraphs [4.89]–[4.100].

33 Chapter 4 at paragraphs [4.4]–[4.5].

34 New Zealand Police *Guidelines for conducting strip searches* (January 2012). These guidelines are required by s 126 of the Search and Surveillance Act 2012 and are available on the Police website.

35 The policy statements concerning public surveillance are discussed in Chapter 11 at paragraphs [11.28]–[11.71]. As we explain in that chapter we use the term “public visual surveillance” to refer to the use of visual surveillance technology in circumstances not requiring a surveillance warrant. We use the phrase “social media monitoring” to refer to enforcement officers accessing social media platforms to obtain information about individuals or classes of individuals. Finally, by “directed surveillance” we mean observation or monitoring of an individual’s movements or activities in circumstances not requiring a surveillance warrant. This would include activity by enforcement officers such as “stake-outs” of a person’s house or following a suspect in a car.

36 Chapter 9 at paragraphs [9.32]–[9.33] and [9.64].

37 Chapter 15 at paragraphs [15.125]–[15.128]. “Covert operations” is a broad term that covers operations in which an enforcement officer or another person acting at the direction of an enforcement agency establishes, maintains or uses a relationship with any other person for the covert purpose of obtaining information by deception (for example, by not disclosing their true motive or identity).

38 See the discussion of this problem and our proposed policy statement in Chapter 14 at paragraphs [14.65]–[14.85].

Surveillance warrants

- 37 In light of developments in technology, we recommend that the Act should no longer refer to surveillance devices and should instead refer to “surveillance technology”.³⁹ This will ensure that warrants are required, and available, to carry out surveillance using intangible technologies (such as computer programs) rather than devices.
- 38 We also recommend that the surveillance warrant regime in the Act should be extended to enable data surveillance.⁴⁰ Data surveillance includes logging a computer user’s keystrokes on a keyboard and monitoring their web browsing history. We consider that the Act should treat data surveillance as involving the same level of intrusion as interception. As such, the same threshold for obtaining a warrant should apply.

Access to passwords and encryption keys

- 39 We envisage that the availability of keystroke logging technology in particular could assist enforcement officers in obtaining the passwords and encryption keys that are necessary to gain access to electronic devices. To further assist in this task, we recommend that the Act should be amended to clarify that the privilege against self-incrimination can only be relied upon to refuse a request from an enforcement officer to provide the access information for a device in very limited circumstances. In addition, we recommend that the penalty for refusing to provide this assistance should be increased.⁴¹

Search and surveillance in urgent circumstances

- 40 We recommend amendments to make it easier for enforcement officers to carry out surveillance without a warrant where it is necessary to prevent offending or avert an emergency.⁴² We also recommend that new warrantless search and surveillance powers should be enacted to assist in locating any high-risk offender who is subject to electronic monitoring as a condition of parole or an extended supervision order and absconds after tampering with their monitoring device.⁴³ We consider these powers are necessary to allow Police to effectively protect the safety of the public.

Searches of electronic devices

- 41 Over the last five years, electronic devices (such as smartphones) have become increasingly prevalent and sophisticated. The owners of such devices have a high privacy interest in their contents. This has been recognised in New Zealand and international case law.
- 42 In light of this case law, we recommend the Act should be amended to enable a police officer executing a warrantless search power to seize and secure, but not search, an electronic device. We think that, to search an electronic device, the Act should require an enforcement officer to obtain a search warrant, unless it is an urgent situation.⁴⁴

Internet searches

- 43 Internet searches are problematic. First, they raise a difficult issue of jurisdiction. If data is stored on a server overseas, it could be a breach of customary international law and/or the law

39 Chapter 7 at paragraphs [7.21]–[7.26].

40 Chapter 7 at paragraphs [7.37]–[7.55]. “Data surveillance technology” refers to a device, program or other technological aid capable of being used to monitor or record the input of information to, or output of information from, an electronic device.

41 Chapter 12 at paragraphs [12.154]–[12.179].

42 Chapter 7 at paragraphs [7.61]–[7.66].

43 Chapter 7 at paragraphs [7.61]–[7.66] and Chapter 13 at paragraphs [13.25]–[13.29].

44 Chapter 12 at paragraphs [12.39]–[12.43].

of the foreign State to access it from New Zealand without that State's consent. Second, the provisions in the Act governing Internet searches are open to different interpretations, and the practices of enforcement agencies vary.

- 44 We recommend redrafting the current provisions to clarify their effect.⁴⁵ However, our primary recommendation in this area reiterates a recommendation the Law Commission made in 2007: consideration should be given to acceding to the Budapest Convention (the leading international agreement dealing with cybercrime).⁴⁶ The parties to this Convention are currently considering what the appropriate international response to the problems posed by Internet searches should be.
- 45 To facilitate the process of accession, we also recommend that the Act should be amended to include a preservation regime.⁴⁷ Having such a regime is a prerequisite for accession to the Convention.

Covert operations

- 46 Covert operations (more often referred to as “undercover” operations) are subject to statutory authorisation regimes in the United Kingdom and in Australia but not in New Zealand.
- 47 We recommend that the Act should be amended to regulate covert operations through a combination of a warrant regime, policy statements and an external auditing process.⁴⁸ To enhance the effectiveness of covert operations, we also recommend that the Act should include a regime for enforcement agencies to obtain assumed identity documents (for example, passports under false names) for use by undercover officers.⁴⁹ We also recommend more comprehensive immunities from prosecution for enforcement officers acting under a covert operations warrant.⁵⁰

Procedural matters

- 48 The Report contains several recommendations that relate to procedural matters. In relation to surveillance, we recommend requiring additional information to be included in applications for interception warrants; permitting entry onto specified properties adjacent to a target property to execute a warrant covertly; providing for removal of surveillance technology; and enabling retention of raw surveillance data that may be relevant for evidential purposes.⁵¹
- 49 We also make recommendations in relation to the notification and reporting requirements that attach to production orders and search warrants.⁵²

45 Chapter 12 at paragraphs [12.125]–[12.153].

46 Chapter 12 at paragraphs [12.95]–[12.103].

47 Chapter 14 at paragraphs [14.145]–[14.150].

48 There is an overview of these recommendations in Chapter 15 at paragraphs [15.83]–[15.87].

49 Chapter 15 at paragraphs [15.146]–[15.150].

50 Chapter 15 at paragraphs [15.140]–[15.145].

51 Chapter 9 at paragraphs [9.46]–[9.50] and Chapter 10.

52 Chapter 14 at paragraphs [14.92]–[14.126].

Clarifications

- 50 There are several aspects of the Act's surveillance provisions that we think would benefit from clarification. For example, we recommend that:
- the Act should clarify that extrasensory surveillance (such as thermal imaging and x-ray) is a form of visual surveillance;⁵³
 - the definitions of the various types of surveillance should explain how any areas of overlap should be addressed;⁵⁴
 - the Act should clarify that tracking ships and aircraft using radar, or tracking a person with their consent, is permissible without requiring a warrant;⁵⁵ and
 - a warrant should be required to intercept any communication that is not publicly available.⁵⁶
- 51 We also recommend that various aspects of the declaratory order regime and the provisions governing privilege in the Act should be clarified.⁵⁷

AREAS WHERE WE DO NOT RECOMMEND REFORM

- 52 In two chapters of our Report, we review specific areas of search and surveillance law but do not recommend that the Act should be amended in any way. Those chapters relate to examination orders (Chapter 16) and obtaining assistance from intelligence agencies (Chapter 18). We have included these chapters in our Report because concerns were raised with us about these areas of law, and it is important to explain our reasoning for leaving the law unchanged.

FURTHER WORK TO BE UNDERTAKEN

- 53 Finally, in relation to a few issues in the Report, we propose that further work should be undertaken to determine the best way forward. These are areas where we were not able to conduct the necessary research or consultation in the time available to us. For example, we suggest that there would be value in re-examining the extent to which the Act (which was designed with law enforcement in mind) can appropriately be applied to regulatory agencies.⁵⁸

53 Chapter 7 at paragraphs [7.27]–[7.36].

54 Chapter 7 at paragraphs [7.52]–[7.55] and Chapter 9 at paragraphs [9.69]–[9.74].

55 Chapter 9 at paragraphs [9.59]–[9.64].

56 Chapter 9 at paragraphs [9.10]–[9.18]. Section 46(1)(a) of the Act currently states that a warrant is required to intercept “a private communication”, but that phrase has proven problematic to apply in practice.

57 See Chapters 6 (declaratory orders) and 17 (privilege).

58 Chapter 2 at paragraphs [2.74]–[2.84].

List of recommendations

CHAPTER 1 INTRODUCTION

RECOMMENDATION

R1 Section 357 of the Act should be repealed.

CHAPTER 2 UNDERLYING THEMES

Privacy

RECOMMENDATION

R2 The reference to marae in the definition of “private premises” in section 3 of the Act should be removed, and subsequent references to “private premises” in the Act should be changed to “private premises and marae”. Those references are in sections 46 (activities for which a surveillance device warrant is required), 47 (some activities that do not require a surveillance device warrant), 172 (information to be included in a report on surveillance device warrants and declaratory orders) and the Schedule (powers in other enactments to which all or part of Part 4 of the Act applies).

CHAPTER 3 THE CASE FOR A PRINCIPLES PROVISION

RECOMMENDATIONS

- R3 A principles section should be inserted into the Act.
- R4 Section 98(2) (relating to requirements for further information) should be amended to permit an issuing officer to require an applicant for a warrant or order to supply further information concerning whether and how any of the principles apply.

CHAPTER 4 THE PRINCIPLES

RECOMMENDATION

- R5 The principles section should provide that:
- (a) enforcement officers and issuing officers must take into account the principle that conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement;

- (b) enforcement officers exercising powers under the Act must take into account the principle that a warrant or order should be obtained in preference to exercising a warrantless power;
- (c) issuing officers and enforcement officers exercising powers under the Act must take into account the principles that:
 - (i) State intrusion into an individual's privacy should be proportionate to the public interest in the investigation and prosecution of the offence or the maintenance of the law;
 - (ii) powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected;
 - (iii) powers under the Act should be exercised having regard to te ao Māori and any other relevant cultural, spiritual or religious considerations;
 - (iv) powers under the Act should be exercised in a manner that minimises the impact on children and vulnerable members of the community; and
 - (v) powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any individual.

CHAPTER 5 POLICY STATEMENTS

RECOMMENDATIONS

- R6 Provisions should be inserted into the Act to require policy statements:
- (a) to be issued in respect of specified classes of activity undertaken by enforcement agencies and in relation to any other class of activity the issuer considers appropriate; and
 - (b) to be consistent with the principles in the Act, the Privacy Act 1993 and any other applicable legislation or case law.
- R7 The Act should require enforcement officers to have regard to policy statements when carrying out any activity to which they apply.
- R8 The current requirement in section 126 for chief executives to issue guidelines on strip searches should be replaced with a requirement to issue a policy statement on strip searches.
- R9 Policy statements relating to Police should be issued by the Commissioner of Police. Policy statements relating to other enforcement agencies should be issued by the chief executive of the relevant agency. The function of issuing policy statements should be non-delegable.
- R10 Before issuing a policy statement, the Commissioner of Police or the chief executive of the relevant agency should be required to consult the Ministry of Justice, the Privacy Commissioner and any other person or organisation they consider appropriate and to have regard to any feedback received.

R11 Policy statements should be published on the Police or relevant agency's website and in any other manner the Commissioner or chief executive considers appropriate. Information should, however, be able to be omitted from a policy statement if there would be grounds for withholding it under the Official Information Act 1982.

R12 Each policy statement should be valid for a maximum of five years.

CHAPTER 6 DECLARATORY ORDERS

RECOMMENDATION

R13 The following amendments should be made to clarify the provisions in the Act that deal with declaratory orders:

- (a) The name "declaratory orders" should be changed to "orders authorising specific activity" or something similar.
- (b) Subsection 65(2) (which states that a declaratory order is advisory in character) should be repealed.
- (c) A new provision should be inserted stating that a declaratory order is invalid if the activity it covers is unlawful or unreasonable.
- (d) The Act should be amended to ensure that section 165(b) (which states that every person is immune from civil or criminal liability for any act done in good faith that is covered by a declaratory order) applies even if the order is later found to be invalid.
- (e) Section 69 should be amended to state that the judge can impose conditions on a declaratory order.
- (f) Sections 98(2) (relating to requirements for further information), 99 (application must be verified), 100 (mode of application for a search warrant), 101 (retention of documents) and 105 (transmission of search warrant) should apply to declaratory orders, with any necessary modifications.

CHAPTER 7 SCOPE OF SURVEILLANCE POWERS

Surveillance not covered by the regime

RECOMMENDATIONS

R14 The Act should be amended to refer to interception, tracking and visual surveillance "technology" as opposed to "devices". This will require amendments to section 46 (activities for which a surveillance device warrant is required) and the definitions of "interception device", "tracking device" and "visual surveillance device" in section 3 of the Act. The definitions should be redrafted in a way that includes the use of computer programs, devices and other technological aids. All references in the Act to "surveillance device warrants" should be replaced with "surveillance warrants".

- R15 The definition of “visual surveillance device” should be amended to clarify that it includes any device or program that can be used to observe private activity by extrasensory means (for example, thermal imaging and x-ray technology).
- R16 The additional restrictions on visual trespass surveillance in sections 45 and 49(5) should apply to any use of visual surveillance technology to observe private activity in private premises.
- R17 The Act should be amended to enable an enforcement officer to obtain a surveillance warrant to use data surveillance technology. The amendments should include the following:
- (a) Inserting a provision defining “data surveillance technology” as a device, program or other technological aid capable of being used to monitor or record the input of information to, or output of information from, an electronic device. The definition should exclude anything that falls within the definition of “interception technology” or “visual surveillance technology”.
 - (b) Amending sections 45 (restrictions on some surveillance), 49(5) (restrictions on who may apply for specified surveillance warrants) and 50 (approval of law enforcement agencies other than Police to carry out specified surveillance) to apply to the use of data surveillance technology in addition to visual trespass surveillance and interception.
 - (c) Amending section 47 (some activities that do not require a warrant under this Part) to provide that an enforcement officer does not require a warrant to use data surveillance technology:
 - (i) to monitor or record inputs or outputs from an electronic device that they are lawfully in possession of; or
 - (ii) in a manner that solely obtains data that is “publicly available”.
- R18 A provision should be inserted into the Act defining “publicly available” as “generally available to members of the public”.

Surveillance for non-evidential purposes

RECOMMENDATIONS

- R19 A new section 48(2)(g) should be inserted to provide that an enforcement officer can carry out warrantless surveillance where they have reasonable grounds:
- (a) to suspect that a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 has tampered with their electronic monitoring device; and
 - (b) to believe that the use of the surveillance technology is necessary to locate that person.

R20 Section 51 (conditions for issuing surveillance device warrant) should be amended to provide that an issuing officer may also issue a warrant if they have:

(a) reasonable grounds:

- (i) to suspect that any one or more of the circumstances set out in section 14(2) exist; and
- (ii) to believe that the use of the surveillance technology is necessary to prevent the offending from being committed or continuing or to avert the emergency; or

(b) reasonable grounds:

- (i) to suspect that a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 has tampered with their electronic monitoring device; and
- (ii) to believe that the use of the surveillance technology is necessary to locate that person.

R21 Section 45 (restrictions on some surveillance) should be amended to provide that the higher threshold for the use of interception and visual trespass surveillance does not apply to the warrantless power in section 48(2)(b) or to the new warrantless and warrant powers outlined in R19 and R20.

CHAPTER 8 AVAILABILITY OF SURVEILLANCE POWERS

RECOMMENDATIONS

R22 Section 50(4) should be amended to add Immigration New Zealand to the list of “specified law enforcement agencies” that may be approved by the Governor-General to carry out visual trespass surveillance and use interception technology.

R23 The Ministry of Justice should consult with enforcement agencies to determine which agencies with warrantless powers should be able to apply for a surveillance warrant or production order and whether that should be provided for in the Act or other legislation.

CHAPTER 9 INTERCEPTION AND TRACKING

Scope of the interception warrant requirement

RECOMMENDATIONS

R24 The definition of “private communication” in section 3 should be repealed. Wherever the term “private communication” is currently used, it should be replaced with “communication”. This will require amendments to the definitions of “intercept” and “interception device” in section 3 and to sections 46(1)(a) and 50(3)(a).

R25 A provision should be inserted into the Act defining “communication” as including “signs, signals, impulses, writing, images, sounds, information, or data that a person or machine produces, sends, receives, processes, or holds in any medium”.

R26 Section 47 should be amended to provide that a warrant is not required to intercept a communication that is publicly available.

Interception with consent

RECOMMENDATIONS

- R27 A provision should be inserted into the Act that requires a policy statement to be issued providing guidance on the use of interception and tracking technology with consent. The statement should include guidance on:
- (a) what amounts to consent, including the procedures for obtaining and documenting consent;
 - (b) precautions that should be taken before carrying out consent surveillance; and
 - (c) any circumstances in which a warrant should be obtained.
- R28 Section 47(1)(b) should be amended to provide that a warrant is not required for an enforcement officer to “intercept a communication between two or more persons made with the consent of at least one of them”.

Incidental interception

RECOMMENDATION

- R29 Section 49 should be amended to require applications for warrants to use interception technology to identify:
- (a) any circumstances the enforcement officer is aware of indicating that the communications of third parties may be incidentally intercepted; and
 - (b) the process that will be followed to monitor and filter intercepted material.

Exceptions to the tracking warrant requirement

RECOMMENDATION

- R30 Section 47 should be amended to provide that a warrant is not required for an enforcement officer to:
- (a) use radar to ascertain the location of ships, boats or aircraft; or
 - (b) track a person with their consent or track a thing with the consent of the person entitled to possession of it.

Relationship between tracking and other surveillance

RECOMMENDATIONS

- R31 A provision should be inserted into the Act stating that an enforcement officer can use tracking technology that also falls within the definition of “interception technology” or “data surveillance technology” under a warrant or power authorising the use of tracking technology only, provided that it will be used in a manner that solely generates location data.
- R32 The definition of “tracking technology” should exclude the use of visual surveillance technology.
- R33 The Act should be amended to include a provision stating that an enforcement officer can obtain location data after the fact pursuant to a production order and that no surveillance warrant is required for this purpose.

CHAPTER 10 SURVEILLANCE: PROCEDURAL MATTERS

Entry to third-party premises

RECOMMENDATION

- R34 The Act should be amended to allow an issuing officer, when issuing a search warrant or surveillance warrant, to authorise entry to premises other than the premises that are the subject of the search or surveillance (third-party premises). The amendments should include the following:
- (a) Inserting a provision that states an issuing officer may authorise entry to third-party premises where they are satisfied the entry is necessary to carry out the authorised search or surveillance without endangering the safety of any person or prejudicing ongoing investigations.
 - (b) Providing that sections 131(1)(a), 131(2), 131(4)–(7) and 134–135 (which contain identification and notice requirements) apply with any necessary modifications where an enforcement officer enters third-party premises. The enforcement officer should explain that they are authorised to cross the property in order to execute a warrant, but should not be required to show the occupier a copy of the warrant or disclose any details about the investigation. The identification and notice requirements should only apply if the entry to third-party premises would amount to a trespass.

Removal of surveillance devices

RECOMMENDATION

- R35 The Act should be amended to provide for the removal of surveillance technology following the expiry of a surveillance warrant. The following provisions should be inserted:
- (a) A provision permitting an enforcement officer to re-enter premises without a warrant to remove surveillance technology within 21 days after the expiry of the warrant that permitted the installation of the device. This power should not apply if the enforcement officer is aware of a significant change in circumstances (such as a change in occupation of the property).
 - (b) A provision empowering a judge to issue a removal warrant authorising re-entry to a property to remove surveillance technology if they are satisfied that the warrant is necessary in the circumstances. The judge should be able to impose conditions setting out how the re-entry should occur.
 - (c) A provision stating that removal warrants are valid for a period of 21 days, but that a further removal warrant may be issued in relation to the same premises if required.

Retention of raw surveillance data

RECOMMENDATION

- R36 Sections 63–64 (which relate to the retention and disposal of raw surveillance data) should be repealed and replaced with a provision that states the following:
- (a) An investigating officer must delete raw surveillance data obtained in relation to a target if they determine that it does not contain any evidential material. “Target” should be defined as a person, place, vehicle or thing specified in the warrant under section 55(3)(d) or a description of the surveillance provided under section 55(4).
 - (b) If raw surveillance data obtained in relation to a target is a mixture of evidential material and data that is not evidential material, it can be retained in its entirety.

CHAPTER 11 PUBLIC SURVEILLANCE

RECOMMENDATIONS

- R37 The Act should require policy statements to be issued in relation to:
- (a) the use of visual surveillance technology in circumstances not requiring a surveillance warrant (“public visual surveillance”);
 - (b) access to social media platforms to obtain information about individuals or classes of individuals (“social media monitoring”); and
 - (c) the observation or monitoring of an individual’s movements or activities in a manner not requiring a surveillance warrant (“directed surveillance”).

- R38 The policy statements covering public visual surveillance, social media monitoring and directed surveillance should include guidance on:
- (a) the purposes for which the activity may be carried out and the types of circumstances in which its use may or may not be appropriate;
 - (b) when a specific warrant or order should be sought;
 - (c) the manner in which the activity should be carried out in order to minimise the level of intrusion on privacy involved;
 - (d) any internal approval, monitoring, reporting and record-keeping requirements that need to be complied with; and
 - (e) requirements as to the use, storage and destruction of information obtained.

CHAPTER 12 DIGITAL SEARCH

A warrant requirement

RECOMMENDATIONS

- R39 Sections 110(h) and 125(l) of the Act (which outline the powers of search) should be amended to remove the ability for a person executing a warrantless search power under Part 2 of the Act to automatically search an electronic device if the device may contain intangible material that is the subject of the search. This should be replaced by a power to seize and secure such a device, pending determination of an application for a search warrant authorising a search of the contents of the device.
- R40 A provision should be inserted into the Act to enable an electronic device that is obtained during the execution of a warrantless search power under Part 2 of the Act to be searched without a warrant in urgent circumstances. The circumstances should align with those described in section 14(2) of the Act.

The content of the warrant

RECOMMENDATIONS

- R41 Section 103(4) (which explains what a search warrant must contain) should be amended to include a statement that every search warrant must contain, in reasonable detail, a description of any computer systems or other data storage devices that may be seized and searched.
- R42 Section 110(h) (which explains that a person exercising a search power may access a computer system or other data storage device) should be amended to permit access only where the device is described in the warrant and may contain intangible material that is the subject of the search.

R43 Section 103(3)(b) (which states that a search warrant may be subject to conditions) should be amended to include a third example of the types of conditions that could be specified in a search warrant. The example should be framed along the following lines: “any condition to minimise the level of intrusion on the privacy of any person likely to be affected during a search, including a search of a computer system or other data storage device”.

Issues raised by Internet searches

RECOMMENDATION

R44 The Government should consider whether New Zealand should accede to the Council of Europe Convention on Cybercrime ETS 185 (Budapest Convention).

The Internet search provisions in the Act

RECOMMENDATION

- R45 The Ministry of Justice should give further consideration to the following:
- (a) Whether the remote access search provisions in the Act should be repealed.
 - (b) Whether the definition of “computer system” in the Act should:
 - (i) be limited so that it only covers computer systems, or the parts of computer systems, that are in New Zealand; and
 - (ii) expressly exclude data that is only accessible when the device is connected to the Internet.
 - (c) Whether provisions should be inserted into the Act to require an enforcement officer to obtain a search warrant with Internet access authorisation before accessing the Internet during a search.
 - (d) Whether provisions should be inserted into the Act to allow an enforcement officer to obtain a search warrant with remote execution authorisation. This authorisation would enable a search warrant that only relates to an Internet search to be executed remotely.
 - (e) Whether provisions should be inserted into the Act to enable an enforcement officer conducting a digital search pursuant to a search warrant to extend that search to internet-based data not specified in the warrant, by exercising a new warrantless power, if they have reasonable grounds to believe:
 - (i) that evidential material relating to the offence is in a place that can be accessed using the Internet; and
 - (ii) that, in the particular circumstances of the case, if access is delayed to obtain a second search warrant, the evidential material will be destroyed, concealed, altered or damaged.

The warrantless power should be subject to a requirement to document the search procedure during or as soon as practicable after the search.

Access information

RECOMMENDATIONS

- R46 Section 130 (duty of persons with knowledge of computer system or other data storage devices or Internet site to assist with access) should be amended to clarify that the privilege against self-incrimination only protects a person from having to disclose the content of access information if the content is itself incriminating. The section should provide that an enforcement officer may require a person to provide any assistance that is reasonable and necessary to access a device or an Internet site.
- R47 The maximum penalty for non-compliance with section 130 of the Act should be increased to six months' imprisonment for an individual or a \$20,000 fine for a body corporate. This will require an amendment to section 178.

CHAPTER 13 WARRANTLESS POWERS

RECOMMENDATION

- R48 A new provision should be inserted into Part 2 of the Act to create a warrantless power, which would allow a constable to enter a property to assist in locating a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 where the constable has reasonable grounds to:
- (a) suspect the person has tampered with the device;
 - (b) believe the device is in the property; and
 - (c) believe the person is not present at the property.

CHAPTER 14 PRODUCTION ORDERS

A production order policy statement

RECOMMENDATION

- R49 A provision should be inserted into the Act requiring a policy statement to be issued in respect of production orders. That statement should contain guidance on how to:
- (a) apply the reasonable expectation of privacy test described in the majority judgment in *R v A* [2017] NZSC 42;
 - (b) prepare appropriately tailored production order applications; and
 - (c) decide whether to apply for a production order or an interception warrant in any given case.

The financial cost of production orders

RECOMMENDATION

- R50 The Ministry of Justice should undertake further work to identify and evaluate the options for establishing a cost contribution scheme in respect of:
- (a) production orders and notices obtained by enforcement officers and directed to service providers; and
 - (b) requests from enforcement officers for service providers to supply customer records on a voluntary basis.

Notification

RECOMMENDATION

- R51 The Act should be amended to include new notification requirements in respect of production orders and search warrants. The amendments should include the following:
- (a) Inserting a provision into the Act to require an enforcement officer to take reasonable steps to notify the target(s) of a production order or a search warrant as soon as possible after the order or warrant has been executed. By “target”, we mean any person whose personal information is a primary or central focus of a production order or search warrant.
 - (b) Inserting a provision into the Act enabling an issuing officer to defer compliance with the notification obligations in respect of a production order for up to 12 months if the notification would endanger the safety of any person or prejudice an ongoing investigation. A second postponement of up to 12 months or a dispensation from compliance should also be available.
 - (c) Amending section 75(2) (which explains what a production order must set out) to state that a production order must set out any period during which compliance with the notification obligation in respect of a production order has been deferred.
 - (d) Amending section 75(1) (which explains what a production order requires the recipient to do) to require the person against whom a production order is made not to disclose the existence of that order to any person who is a target of the order until after any period of deferred notification specified in the order has expired.

Reporting

RECOMMENDATION

- R52 The Ministry of Justice should conduct further work to identify the costs of implementing a requirement for enforcement agencies to report on the number of applications for production orders and search warrants that are granted or refused each year.

A data preservation regime

RECOMMENDATION

- R53 Provisions should be inserted into the Act to introduce a new preservation notice regime. That regime should comply with the requirements outlined in the Budapest Convention. The provisions should:
- (a) Enable the Commissioner of Police, a Deputy Commissioner of Police or an Assistant Commissioner of Police to issue a preservation notice.
 - (b) State that a preservation notice requires the recipient to preserve specified data, on a confidential basis, for no more than 20 days. Where appropriate, the notice may also require the recipient to disclose limited metadata to a specified enforcement officer solely for the purposes outlined in the Budapest Convention.
 - (c) Enable an issuing officer to extend the preservation period for up to 90 days.
 - (d) Enable an enforcement officer who can apply for a production order under the Act and the Competent Authority for mutual assistance in New Zealand to:
 - (i) request that a preservation notice be issued; and
 - (ii) apply for the preservation period to be extended.
 - (e) Provide that a preservation notice can only be issued or the period of preservation extended under the Act if the decision-maker is satisfied that:
 - (i) the relevant enforcement agency intends to apply for a production order in respect of the identified data;
 - (ii) the requirements for obtaining a production order are likely to be fulfilled in the circumstances of the case; and
 - (iii) preservation is necessary because the data is particularly vulnerable to loss or modification.
 - (f) Provide that non-compliance with a preservation notice is an offence.

CHAPTER 15 COVERT OPERATIONS

Covert operations warrants

RECOMMENDATIONS

- R54 A provision should be inserted into the Act to permit an enforcement officer to apply for a warrant to conduct a covert operation.
- R55 “Covert operation” should be defined as an operation in which an enforcement officer or another person acting at the direction of an enforcement agency establishes, maintains or uses a relationship with any other person for the covert purpose of obtaining information or providing another person with access to information.

- R56 The Act should provide that covert operations warrants should:
- (a) Be issued by an independent, impartial and legally-qualified person who can be trusted with sensitive operational information. This role could be performed by High Court judges (subject to consultation with the judiciary) or a commissioner appointed under the Act.
 - (b) Only be issued where there are reasonable grounds to suspect an offence punishable by imprisonment has been, is being or will be committed; and to believe that the operation will obtain evidential material relating to that offence.
 - (c) Not be issued if the operation is likely to seriously endanger the health or safety of any person or result in serious loss of or damage to property (other than property owned by the enforcement agency or unlawful goods).
 - (d) Be capable of being renewed and varied.
 - (e) Be subject to any conditions that the issuing officer considers reasonable.
- R57 The Act should state that covert operations warrants cannot authorise activity for which a surveillance warrant is required.
- R58 Applications for covert operations warrants should include the following information:
- (a) the name of the applicant;
 - (b) the suspected offence in relation to which the warrant is sought or issued;
 - (c) a description of the evidential material believed to be able to be obtained through the operation;
 - (d) the name or other description (such as a code name) of the agent(s) who it is proposed will conduct the operation;
 - (e) the period for which the warrant is sought, up to a maximum of three months;
 - (f) the name, address or other description of the target(s);
 - (g) the period for which the warrant is sought, up to a maximum of three months;
 - (g) a description of the activity it is proposed the agent will carry out; and
 - (h) the circumstances in which the covert operation is intended to be carried out in enough detail to identify the parameters of, and the objectives to be achieved by, the operation, if it is not possible to provide sufficient information to identify the target or describe the evidential material to be obtained.
- R59 Sections 98(2) (relating to requirements for further information), 99 (application must be verified), 100 (mode of application for a search warrant), 101 (retention of documents) and 105 (transmission of search warrant) should apply to covert operations warrants, with any necessary modifications.

Policy statements

RECOMMENDATION

- R60 The Act should require policy statements to be issued in respect of covert operations. Covert operations policy statements should contain guidance on:
- (a) considerations that should be taken into account when deciding whether to initiate a covert operation and how it should be conducted;
 - (b) the situations in which a covert operations warrant should be sought;
 - (c) any matters that should be specifically highlighted in warrant applications;
 - (d) internal planning, approval, monitoring, reporting, record-keeping and evaluation requirements;
 - (e) the processes that will be followed if any potential misconduct by agents or other enforcement officers is identified; and
 - (f) arrangements to protect the safety of agents and others.

External audits

RECOMMENDATION

- R61 The Act should be amended to provide that all warranted covert operations and a selection of non-warranted covert operations should be subject to annual auditing by an external person or body. The auditor should:
- (a) assess whether an operation complied with the applicable policy statement and (where relevant) warrant, and identify any instances of potentially unlawful or unreasonable conduct;
 - (b) have broad powers to access any relevant operational information;
 - (c) report to the House of Representatives annually on the outcome of the audit; and
 - (d) refer any case involving a potential irregularity to the Independent Police Conduct Authority, in the case of Police, or to the responsible Minister, in the case of other enforcement agencies.

Immunities

RECOMMENDATIONS

- R62 A provision should be inserted into the Act stating that any person is immune from civil liability and from criminal liability for the commission of specified offences for any act done in good faith in relation to the execution of a covert operations warrant, provided the execution is carried out in a reasonable manner.
- R63 Section 167 (immunity of the Crown) should be amended (if required) to apply to the new immunity in respect of covert operations warrants.

Assumed identity information

RECOMMENDATION

- R64 The Act should be amended to include an assumed identity regime for Police similar to that contained in the Intelligence and Security Act 2017. The Ministry of Justice should consult other agencies that conduct covert operations to determine whether the regime should apply to their officers in whole or part.

CHAPTER 17 PRIVILEGE

RECOMMENDATIONS

- R65 The reference to production orders in section 138 (privilege against self-incrimination) should be removed.
- R66 Provisions should be inserted into the Act to require production orders and examination orders to contain an explanation of the availability of relevant privileges and an outline of how those privileges may be claimed.
- R67 A provision should be inserted into the Act to clarify that claims to privilege do not require resolution by a court if the enforcement agency and the privilege owner agree to exclude certain material from the search and agree on a procedure for isolating that material.



Part 1
OVERARCHING
ISSUES

Chapter 1

Introduction

ORIGINS OF THE SEARCH AND SURVEILLANCE ACT 2012

The Law Commission's original Report

- 1.1 In 2007, the Law Commission published *Search and Surveillance Powers*, its Report on the law relating to the search, seizure and surveillance powers of law enforcement agencies. The Report was described by the Commission as its most substantial piece of work in its then 21-year history.¹ It had taken half a decade.
- 1.2 The Commission noted that the incremental development of search and surveillance powers meant they were scattered across the statutory landscape and were often inconsistently designed, with differing thresholds for their exercise. It also recognised that the powers were not designed to accommodate new technology and that rapidly developing surveillance devices were only partially regulated.
- 1.3 The 2007 Report therefore made 300 recommendations aimed at consolidating the law of search and surveillance and bringing it within a framework that balanced law enforcement and human rights values. It addressed the exercise of powers that required a threshold of belief or suspicion as to the commission of an offence before they can be exercised. It did not focus on search or inspection powers designed to monitor compliance with regulatory regimes – where often no such threshold is required.²

The legislative response

- 1.4 In September 2008, the Labour Government introduced the Search and Surveillance Powers Bill,³ the first legislative response to the Commission's work. That Bill was discharged from the legislative process in July 2009.
- 1.5 The Search and Surveillance Bill 2009 (which was ultimately enacted) was introduced by the then National Government.⁴ The Bill had an extended Select Committee process that began in August 2009. A year later, the Committee issued an interim report. It attached to that report a lengthy departmental report produced by the Ministry of Justice and the Law Commission, which included an analysis of the submissions that had been made during the consultation process.⁵ The Committee then called for further written submissions. The final Select Committee Report presented in November 2010 contained a substantial redraft of the Bill.⁶
- 1.6 In March 2012, the Bill was read for a second time, progressed to the Committee of the Whole House (where an extensive supplementary order paper containing further proposed changes

1 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at 15.

2 At 20.

3 Search and Surveillance Powers Bill 2008 (300-1).

4 Search and Surveillance Bill 2009 (45-1).

5 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010).

6 Search and Surveillance Bill 2009 (45-2).

was introduced) and then had its third reading. The Bill received the Royal assent in April, and some of its provisions came into force on 18 April 2012. Most of the remainder became operative on 1 October 2012.

- 1.7 The Act, unlike the original Law Commission recommendations, covers the manner in which some regulatory search powers are exercised. Accordingly, certain parts of the Act are addressed to all “enforcement officers”,⁷ which includes both constables and other people with law enforcement or regulatory powers listed in the Schedule to the Act.⁸

THE STATUTORY REQUIREMENT TO CONDUCT A REVIEW

- 1.8 Section 357 of the Search and Surveillance Act 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.
- 1.9 The rationale behind this provision was explained in the departmental report as follows:⁹
- [Section 357] 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.
- 1.10 In accordance with section 357 of the Act, the Minister of Justice asked the Law Commission and the Ministry of Justice to commence our review on 28 June 2016.
- 1.11 Our terms of reference (included in Appendix 1) incorporate the wording of section 357, with an additional question that arose out of the report of the First Independent Review of Intelligence and Security, delivered in February 2016.¹⁰

THE REVIEW PROCESS

- 1.12 We began our review with numerous preliminary meetings with enforcement agencies to scope issues—from a law enforcement or regulatory compliance perspective—that had arisen with the

7 “Enforcement officer” is defined in s 3 of the Search and Surveillance Act 2012 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.

8 See the discussion of regulatory search powers in Chapter 2 at paragraphs [2.74]–[2.84].

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

10 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).

Act's operation. We also reviewed relevant case law and engaged with other organisations and interested parties to isolate issues that might benefit most from public consultation.

- 1.13 We established two groups with whom we formally engaged at different stages of our review process. The first was our Officials Group, which included representatives from enforcement agencies who are daily users of the legislation. The second was our Expert Advisory Group. Its members were selected for their expertise in privacy law, human rights, criminal law, technology and digital security.
- 1.14 Before writing our Issues Paper, we met with our Officials Group to seek preliminary comments on the questions we had formulated for public consultation.
- 1.15 Our Issues Paper, *Review of the Search and Surveillance Act 2012*, was published on 8 November 2016 on the Commission's website, and submissions were sought.¹¹ In addition, the Ministry of Justice's online consultation hub¹² was used. This reflected the joint nature of the review and provided an alternative method for the public to engage with the questions raised in our Issues Paper.
- 1.16 We received 31 formal submissions or comments from a range of enforcement agencies, other government bodies, the legal profession, issuing officers, private organisations/industry bodies and individual members of the public.
- 1.17 Based on those submissions and our own research and analysis, the review team formed preliminary views on proposals for this Report, which were discussed during meetings with our Expert Advisory Group and Officials Group. The feedback we received has informed the recommendations in this Report.

THE STRUCTURE OF THIS REPORT

- 1.18 Part 1 of our Report discusses overarching issues and consists of Chapters 1 to 6. Chapter 2 outlines the underlying themes and issues that have informed our thinking during this review. Chapters 3, 4 and 5 deal with principles and policy statements. In Chapter 6, we discuss declaratory orders and whether they should be replaced with a residual warrant regime to better accommodate future developments in technology.
- 1.19 The next five chapters in our Report form Part 2 and relate to surveillance. Chapter 7 examines the current scope of surveillance powers and whether the Act should enable additional powers to be used. Chapter 8 looks at whether surveillance warrants should be more widely available and who they should be issued by. We look at the specific issues that are raised by interception and tracking in Chapter 9, and Chapter 10 addresses procedural matters. In Chapter 11, we discuss public surveillance, which includes the use of CCTV footage and social media monitoring.
- 1.20 Part 3 of the Report focuses on search powers. Chapter 12 discusses whether the Act should be amended to provide clearer rules around searches of electronic devices and Internet searches. Chapters 13 and 14 then discuss warrantless search powers and production orders.
- 1.21 In Part 4 of the Report, we discuss two other investigative methods: covert operations (Chapter 15) and examination orders (Chapter 16). Finally, Part 5 of the Report discusses whether the

11 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016). Submissions were sought by 16 December 2016, but we continued to accept submissions in January 2017.

12 < <https://consultations.justice.govt.nz/> > .

provisions in the Act dealing with privilege need to be amended (Chapter 17) and answers a discrete question concerning the intelligence agencies (Chapter 18).

Glossary of frequently used terms

- 1.22 We use a number of specific terms in this Report 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 2).

FUTURE REVIEWS OF THE ACT

- 1.23 Finally, we note that during the course of our consultation, it was suggested to us by a member of our Expert Advisory Group that the Law Commission and the Ministry of Justice should review the operation of the Act every five years. It was suggested that this was necessary in order to address any new surveillance techniques that may develop over time.
- 1.24 We can see value in ongoing monitoring of the Act, as it will no doubt require further updating as technology and investigatory methods develop. However, in our view, it is preferable for the Ministry of Justice to address issues as they arise rather than through legislatively mandated reviews. For that reason, we do not recommend the Act be amended to require continuing statutory reviews of the Act, which would have significant resource implications. Instead, we recommend that section 357 of the Act should be repealed given that it no longer serves a purpose in the legislation.
- 1.25 As we go on to explain in Chapter 5, we recommend that chief executives of enforcement agencies¹³ be required to issue policy statements in relation to a number of types of search and surveillance activity and that those statements are developed in consultation with the Ministry of Justice.¹⁴ In our view, the Ministry's involvement in the preparation of policy statements will help to ensure it is kept informed of areas where the Act is falling behind developments in technology and investigatory methods. The Ministry can, if necessary, brief the Minister of Justice, who can propose changes to the Act as required.

RECOMMENDATION

- R1 Section 357 of the Act should be repealed.

13 “Enforcement agency” is defined in s 3 of the Search and Surveillance Act 2012 as any department of State, Crown entity, local authority, or other body that employs or engages enforcement officers as part of its functions. See also Chapter 2 at paragraphs [2.75]–[2.85].

14 Chapter 5 at paragraphs [5.33]–[5.35].

Chapter 2

Underlying themes

INTRODUCTION

- 2.1 In this chapter, we identify particular themes and issues that have informed our thinking during this review. Our aim is to provide greater context to our analysis of the issues raised in this Report and to illustrate how search and surveillance has changed since the publication of the Law Commission’s 2007 Report, *Search and Surveillance Powers*.¹
- 2.2 The themes and issues explored in this chapter are:
- the values underpinning the Search and Surveillance Act 2012 (the Act), particularly privacy and effectiveness, and how these have developed in the last ten years;
 - the relationship between the Act and section 30 of the Evidence Act 2006, as illustrated by recent case law; and
 - the relationship between law enforcement and regulatory powers, and problems that have arisen from the application of aspects of the Act to some regulatory powers.
- 2.3 We also briefly discuss the concept of informed consent, as it arises in the context of a number of issues discussed in this Report.

VALUES UNDERPINNING THE ACT

- 2.4 Section 5 of the Search and Surveillance Act provides the starting point for considering the values underpinning the legislation. That section states that the main purpose of the 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”.²
- 2.5 It is clear that human rights values and law enforcement values both arise in the context of regulating search and surveillance powers. These two sets of values were explored in some detail in the Law Commission’s 2007 Report.³ The Commission made two preliminary observations. First, it did not see law enforcement values and human rights values as necessarily competing with one another:⁴

[W]hile 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 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007).

2 Search and Surveillance Act 2012, s 5.

3 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) ch 2.

4 At [2.7].

- 2.6 Second, the Commission observed that the purpose of exploring the two sets of values was to assist analysis, not to “dictate the correct answer in every case”.⁵ It considered that a principled, values-based approach to search and surveillance powers was the best way to achieve consistent protection of human rights yet promote effective law enforcement.⁶
- 2.7 The Commission identified the particular human rights and law enforcement values that it believed a search and surveillance regime should reflect. It noted that the principal expression of human rights values in the search and surveillance context is section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA), which guarantees the right of everyone “to be secure from unreasonable search or seizure, whether of the person, property, or correspondence, or otherwise”.⁷ Against that backdrop, the Commission identified the following human rights values engaged by search and surveillance powers:⁸
- the protection of privacy;
 - the protection of personal integrity;
 - the protection of property rights; and
 - the maintenance of the rule of law.
- 2.8 In relation to law enforcement values, the Commission identified the following:⁹
- effectiveness;
 - simplicity;
 - certainty;
 - responsiveness to different types of operational circumstances; and
 - framing search powers in a manner that is human rights consistent.
- 2.9 Each of these values is complex and multifaceted, and we do not intend to provide a comprehensive review of them in this chapter. Instead, we have chosen to focus on two values in particular that we consider are the most complex and relevant to this review: privacy values and effectiveness.

PRIVACY

What is privacy?

- 2.10 It should be noted that the discussion of privacy in this chapter is undertaken in the specific context of law enforcement powers. Wider notions of privacy arise where claims of privacy are made by one citizen against another.¹⁰
- 2.11 In 2007, the Law Commission described privacy as the key human rights value implicated by search and surveillance.¹¹ However, “privacy” is an elastic and complex concept that is notoriously difficult to define. The concept of privacy has been described as a “sweeping

5 At [2.8].

6 At [2.8].

7 At [2.10].

8 At [2.11].

9 At [2.26].

10 A broader exploration of privacy values was conducted by the Law Commission in its four-part review on the law of privacy from 2002–2011 (see in particular Law Commission *A Conceptual Approach to Privacy* (NZLC MP19, 2007) and *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008)).

11 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [2.12]. See also *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 (CA) at [236] per William Young P and Glazebrook J: “[t]he main aim of s 21 of the Bill of Rights is to protect privacy interests”.

concept”,¹² “highly varied and vague”,¹³ and “a nebulous concept that has manifested in several distinct rights and freedoms”.¹⁴ Some commentators have expressed the view that privacy is an unsatisfactory term in that it has “a protean capacity to be all things to all lawyers”.¹⁵

- 2.12 The authors of *Privacy Law in New Zealand* suggest that privacy involves a number of separate but related interests, including:¹⁶
- an interest in controlling entry to one’s personal space;
 - an interest in freedom from interference with one’s person;
 - an interest in controlling information about one held or used by others;
 - an interest in freedom from surveillance and from monitoring or interception of one’s communications;
 - an ability to exclude intrusions that force one to direct attention to the intrusions rather than to matters of one’s own choosing;
 - an interest in freedom from monitoring of one’s associations, including religious and other assemblies; and
 - according to some United States commentators, an interest in freedom to decide on lifestyle, sexual orientation and other personal matters without undue interference.
- 2.13 In a 2008 Study Paper, *Privacy: Concepts and Issues*,¹⁷ the Law Commission adopted a conceptual approach to privacy that it described as a “core values” approach. The Commission suggested that it is possible to conceptualise privacy as a subcategory of two, interconnected core values: the autonomy of humans to live a life of their choosing; and the equal entitlement of people to respect.¹⁸ The Commission also took the view that privacy has two main dimensions:¹⁹
- informational privacy, which is concerned with control over access to private information or facts about ourselves; and
 - local or spatial privacy, which is concerned with control over access to our persons and to private spaces (typically in the home but in other places as well).²⁰

12 Daniel Solove “Conceptualizing Privacy” (2002) 90 Cal L Rev 1087 at 1088. Solove suggests that all attempts to conceptualise privacy by locating a common denominator to identify all instances of privacy have, so far, been unsatisfying: at 1092.

13 James Waldo, Herbert Lin and Lynette Millett (eds) *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washington DC, 2007) at 53.

14 Petra Butler “The Case for a Right to Privacy in the New Zealand Bill of Rights Act” (2013) 11 NZJPIL 213 at 213.

15 See Tom Gerety “Redefining Privacy” (1977) 12 Harv Civil Rights-Civil Liberties L Rev 233 at 234.

16 Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) at [1.1.3].

17 Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008).

18 At [3.10].

19 At [3.15], [3.16] and [3.21]. Another approach, adopted in Canadian case law, is to recognise three categories of protection: informational privacy, bodily privacy and territorial privacy (see *R v Spencer* 2014 SCC 43, [2014] 2 SCR 212 at [35]). The Canadian courts have tended to afford the strongest protections to bodily and territorial privacy. Protection for informational privacy is afforded only when the information in question is part of “a biographical core of personal information which ... tends to reveal intimate details of the lifestyle and personal choices of the individual” (see *R v Plant* [1993] 3 SCR 281 at 293).

20 See also *United States v Jones* 132 S Ct 945 (2012), where the United States Supreme Court held that installing a Global Positioning System tracking device on a vehicle to monitor its movements on public streets was unconstitutional.

Why is privacy important?

2.14 Most commentators agree that privacy is important because “it promotes a number of other ends which are essential for human flourishing”.²¹ Nicole Moreham suggests there are six rationales for protecting privacy:²²

- to protect human dignity;
- to promote individual autonomy;
- to facilitate individual freedom of expression and promote societal discourse;
- to protect intimate and social interaction;
- to preserve health and well-being; and
- to shield individuals from judgement and discrimination.

2.15 Moreham describes the protection of dignity as an objective that both complements and transcends the other rationales.²³ She notes that the relationship between privacy and dignity has been recognised by a number of other commentators²⁴ as well as the judiciary.²⁵ For example, in *Hosking v Runting*, Tipping J said that “[i]t is the essence of the dignity and personal autonomy and wellbeing of all human beings that some aspects of their lives should be able to remain private if they so wish”.²⁶ Similarly in *Brooker v Police*, Thomas J (dissenting) observed that:²⁷

Probably [no human right] is more basic to human dignity than privacy. It is within a person’s sphere of privacy that the person nurtures his or her autonomy and shapes his or her individual identity. The nexus between human dignity and privacy is particularly close.

2.16 Moreham notes that the promotion of individual autonomy is commonly identified alongside dignity as a second reason for protecting privacy.²⁸ She explains that the relationship between privacy and autonomy is not just about respect for individual choice. It also promotes autonomous thought and action.²⁹ In other words:³⁰

[B]y allowing individuals to retreat from the observation of others, privacy creates a zone where people can be free from concern about the judgment of others, ‘be themselves’, and think and act in accordance with their own ideas and principles.

21 Nicole Moreham “Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort” in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation* (LexisNexis NZ Ltd, Wellington, 2008) 231 at 233.

22 Nicole Moreham “The Nature of the Privacy Interest” in Nicole Moreham and Sir Mark Warby (eds) *Tugendhat and Christie’s The Law of Privacy and the Media* (3rd ed, Oxford University Press, Oxford, 2016) 42 at 64–77. See also Moreham “Why is Privacy Important?”, above n 21, at 233.

23 Moreham “Why is Privacy Important?”, above n 21, at 234.

24 See, for example, Edward Bloustein “Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser” (1964) 39 NYU L Rev 962; Samuel Warren and Louis Brandeis “The Right to Privacy” (1890) 4 Harv L Rev 193; and Harry Kalven Jr “Privacy in Tort Law – were Warren and Brandeis Wrong?” (1966) 31 Law & Contemp Prob 326. Some commentators, however, suggest that the notion of dignity cannot justify any right to privacy because it is “fundamentally incoherent”: see, for example, Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (The Federation Press, Sydney, 2005) at 27. John Burrows suggests that dignity does not “by any means” provide the whole explanation for privacy protection, because privacy is capable of protecting a wide range of interests: John Burrows “Invasion of Privacy – *Hosking* and Beyond” (2006) NZ L Rev 389 at 390.

25 Moreham “The Nature of the Privacy Interest”, above n 22, at 65. See also the observations in Stephen Todd and others (eds) *The Law of Torts in New Zealand* (7th ed, Thomson Reuters, Wellington, 2016) at [17.3].

26 *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [239].

27 *Brooker v Police* [2007] 3 NZLR 91 (SC) at [182]. See also at [252].

28 Moreham “The Nature of the Privacy Interest”, above n 22, at 68.

29 At 69.

30 At 69.

Privacy protection in search and surveillance

- 2.17 In the search and surveillance context,³¹ the concept of privacy was traditionally equated with the protection of property rights. The right not to be subjected to unreasonable search and seizure (now reflected in section 21 of NZBORA) has its origins in the common law, which protected individuals against trespassory interferences by State actors with their property rights or bodily integrity.³²
- 2.18 A more modern conception of privacy became apparent in the late twentieth century. In New Zealand, the 1993 decision *R v Jefferies*³³ signalled a shift towards a broader notion of privacy, aimed at protecting individuals from State intrusions on reasonable expectations of privacy.³⁴ The Court of Appeal stated that the interests guarded by section 21 of NZBORA were broader than the mere protection of property rights. In one of five separate judgments,³⁵ Thomas J considered that section 21 was concerned to protect “those values or interests which make up the concept of privacy”.³⁶ Richardson J stressed that a search of the person or premises not only invaded property rights, but also constituted “a restraint on individual liberty, an intrusion on privacy and an affront to dignity”.³⁷
- 2.19 More recently, in *Hamed v R*,³⁸ Blanchard J described the two-step process that a court must engage in when considering whether there has been an unreasonable search or seizure under section 21. The court must ask whether what occurred was a search or seizure, and if so, whether that search or seizure was unreasonable.³⁹
- 2.20 Blanchard J concluded that there would be a “search” where activity “invades a reasonable expectation of privacy”.⁴⁰ His Honour considered there were two elements to this inquiry:⁴¹
- whether the person affected subjectively had such an expectation; and
 - whether the expectation was one that society is prepared to regard as reasonable.
- 2.21 In *Lorigan v R*, the Court of Appeal noted that it was not entirely clear whether there was majority support for Blanchard J’s approach in the other *Hamed* judgments. However, the Court

31 It should be noted that the protection of privacy in New Zealand law is (primarily) manifested in constitutional law (through s 21 of the New Zealand Bill of Rights Act 1990) and tort law, through the recognition of a tort of invasion of privacy (see *Hosking v Runting* [2005] 1 NZLR 1 (CA)) and the more recent recognition of the tort of intrusion into seclusion (see *C v Holland* [2012] 3 NZLR 672 (HC)). The authors of *The Law of Torts in New Zealand* adopt the terminology of the Law Commission and describe the *Hosking v Runting* tort as involving “informational privacy” (because it is concerned with wrongful publicity of information) and the *C v Holland* tort as involving “spatial privacy” (because the tort does not depend on the publication of information about the plaintiff, but rather on invasion of the plaintiff’s private space): Todd and others, above n 25, at [17.6.01].

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

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

34 This is also the approach adopted by the courts in the United States and Canada: see, for example, *R v Wise* [1992] 1 SCR 527 at 533; *Hunter v Southam Inc* [1984] 2 SCR 145 at 159; and *Katz v United States* 389 US 347 (1967) at 360–361.

35 All five judgments agreed on the result (that the evidence was admissible in that case) and dismissed the appeal.

36 *R v Jefferies* [1994] 1 NZLR 290 (CA) at 319.

37 At 302 per Richardson J. See also *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 (CA) at [48] (“[a] touchstone of s 21 of the Bill of Rights is the protection of reasonable expectations of privacy”) per William Young P and Glazebrook J.

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

39 At [162]. It should be noted that legality and reasonableness, while related, are distinct concepts. For example, an unlawful search can nevertheless be reasonable (for example, where the illegality arose as a result of a technical or inconsequential procedural breach or in the case of an emergency); and a lawful search may nonetheless be unreasonable (for example, where a lawful search was conducted in an unreasonable manner). See *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [12], [24] and [226] per William Young P and Glazebrook J; and *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [161] per Blanchard J, affirming the principles in *R v Jefferies* [1994] 1 NZLR 290 (CA).

40 At [163].

41 At [163]. 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 s 21 of the New Zealand Bill of Rights Act 1990, unreasonable: at [163].

- concluded that the test of “state intrusion into reasonable expectations of privacy” was broadly consistent with the *Hamed* judgments and should be applied.⁴²
- 2.22 Despite this acceptance that section 21 of NZBORA protects a wider notion of privacy—reasonable expectations of privacy—two points are worth emphasising.
- 2.23 First, a privacy-based interpretation of “search” does not mean that all intrusions on privacy will breach section 21.⁴³ Section 21 protects only against unreasonable searches, not searches in general. This recognises that there are competing interests that may sometimes outweigh a privacy claim.⁴⁴
- 2.24 Second, it is worth noting that privacy is not explicitly recognised in NZBORA as a stand-alone right. The White Paper on the proposed Bill of Rights Act stated that it would be “inappropriate to attempt to entrench a right that is not by any means fully recognised now, which is in the course of development, and whose boundaries would be uncertain and contentious”.⁴⁵
- 2.25 Privacy values nevertheless underpin not only section 21, but also the right to freedom of thought, conscience and religion (in section 13), the right to freedom of association (in section 17), the right not to be subjected to medical experimentation (in section 10) and the right to refuse to undergo medical treatment (in section 11).⁴⁶ Furthermore, the long title to NZBORA states that it is “an Act to affirm New Zealand’s commitment to the International Covenant on Civil and Political Rights”. New Zealand has therefore committed itself, at an international level, to ensure that no one is subject to “arbitrary or unlawful interference with his privacy, family, home or correspondence”⁴⁷ and to ensure that everyone has the “right to the protection of the law against such interference or attacks”.⁴⁸
- 2.26 Our review has not considered whether New Zealand should recognise a stand-alone right to privacy,⁴⁹ as we consider that issue to be outside the scope of our terms of reference. Instead, we have sought to frame our recommendations in a manner that is consistent with the existing human rights provisions in NZBORA.

Māori conceptions of privacy

- 2.27 An important element of the context in which privacy should be assessed in New Zealand is te ao Māori (the Māori dimension).
- 2.28 The importance of protecting human dignity (discussed above at [2.15]) is a value that is central to both human rights and Māori custom.⁵⁰ The Māori concept that embodies this value is often expressed as respect for the mana (personal power or standing) of each individual. While levels

42 *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22]. The Supreme Court declined leave to appeal the Court’s decision in *Lorigan*, describing it as a “straightforward and unsurprising application ... of a decision of [the Supreme Court]”: *Lorigan v R* [2012] NZSC 67 at [2]. See also *Maihi v R* [2015] NZCA 438 at [20] and, more recently, *R v A* [2017] NZSC 42 at [50].

43 See Paul Rishworth and others *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) at 422.

44 Waldo, Lin and Millett, above n 13, at 319.

45 Geoffrey Palmer *A Bill of Rights for New Zealand: A White Paper* (Department of Justice, Wellington, 1985) at [10.144].

46 Section 28 of the New Zealand Bill of Rights Act 1990 also provides that an existing right or freedom is not abrogated or restricted because it is not included (or fully included) in the Act.

47 International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976), art 17.1.

48 Article 17.2. See also *SF v R* [2014] NZCA 313 at [23].

49 For a discussion on the potential impact of recognising a right to privacy in New Zealand, see Butler “The Case for a Right to Privacy”, above n 14.

50 See Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008) at [5.21] and Law Commission *Converging Currents: Custom and Human Rights in the Pacific* (NZLC SP17, 2006) at 12 and at [4.42].

- of mana differ between individuals, all people possess a mana that should be respected by others.⁵¹
- 2.29 While no Māori concept can be directly equated with the English words “privacy” or “private”, it has been suggested that the Māori concept most closely analogous to the idea of privacy is tapu – a concept that defines things that are special or restricted, including the human person, information, places and objects.⁵² Tapu has been described by Sir Hirini Moko Mead as “a personal force field which can be felt and sensed by others”.⁵³ He notes that violation of this space can cause discomfort, affront and damage.⁵⁴ In contrast to tapu, the complementary concept of noa denotes “a state of relaxed access, requiring no particular protective mechanisms or restrictions”.⁵⁵ Both tapu and noa, then, may have functioned to protect aspects of privacy traditionally and may continue to have some influence on how Māori think about privacy today.⁵⁶
- 2.30 While there are some similarities in Māori and Pākehā conceptions of privacy, it has been suggested that a significant difference is that Māori are more likely to place emphasis on collective, rather than solely individual, interests.⁵⁷
- 2.31 Khylee Quince suggests that differences in cultural perspectives can sometimes create a “chasm” between what Māori and Pākehā consider to be “public” and “private” places and information.⁵⁸ She refers to the status of a marae as an example of the difficulties in viewing one culture through the lens of another. For example, in *R v Iti*,⁵⁹ the Court of Appeal considered whether an area within a marae,⁶⁰ the ātea, was a public or private place (for the purposes of determining whether a charge of unlawfully carrying a firearm in a public place had been established). The Court rejected the argument that the ātea should be seen as a separate, private area. Following English authority,⁶¹ the Court held that the marae formed a single unit, so the whole area (despite containing areas of both public and private access) was to be considered a public place.⁶² Quince observes that the Court appeared to assume the marae was a public place with some restricted or private areas within it, while others might see the marae as a private place with some exceptions. Others still, she suggests, might say that neither argument is correct: rather, the marae is tapu.⁶³
- 2.32 In our view, there is an inherent difficulty in seeking to protect and advance Māori concepts of privacy through the use of English (and legal) terminology. Binary classifications such as “public” or “private” cannot capture the essence of Māori values and norms. There is no easy solution to these challenges; however, we consider that—as far as possible—the terminology

51 Hirini Moko Mead *Tikanga Māori: Living by Māori Values* (Huia, Wellington, 2016) at 33–34 and at 55–57.

52 Khylee Quince “Māori Concepts and Privacy” in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) at [2.1].

53 Mead, above n 51, at 51.

54 At 53.

55 Mason Durie *Whaiora: Māori Health Development* (Oxford University Press, Melbourne, 1994) at 10.

56 Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008) at [5.22].

57 Quince “Māori Concepts and Privacy”, above n 52, at [2.2.1]. Quince explains that, “[f]or Māori, the individual is defined by membership of whānau, hapū and iwi, but he or she retains a sense of self over his or her body, personality, possessions and mana, and over these things may be said to have some privacy. The tapu of the human person ... reflects this notion of individual privacy, while the tapu of places and things are often managed in a manner that demonstrates group privacy”: at [2.2.1].

58 At [2.3.1].

59 *R v Iti* [2007] NZCA 119, [2008] 1 NZLR 587.

60 The marae encompasses the whole complex of land, buildings and facilities at a particular site.

61 *Anderson v Miller* (1976) 64 Cr App R 178 (CA).

62 *R v Iti* [2007] NZCA 119, [2008] 1 NZLR 587 at [37]–[38].

63 Quince “Māori Concepts and Privacy”, above n 52, at [2.3.1].

used in the Search and Surveillance Act 2012 should avoid the re-classification of Māori customs, values and institutions.

- 2.33 This point was made in a submission we received from Te Hunga Rōia Māori o Aotearoa.⁶⁴ It considered the current inclusion of marae in the definition of “private premises” in section 3 of the Act was problematic, because the status of a marae does not fit neatly into the public/private divide. Te Hunga Rōia was nevertheless of the view that marae should be afforded the same protection under the Act as private premises. We agree. We therefore recommend removing the reference to marae in the definition of “private premises” and by changing subsequent references to “private premises” in the Act to “private premises and marae”.⁶⁵

Societal attitudes towards privacy

- 2.34 In its 2008 Study Paper, *Privacy: Concepts and Issues*,⁶⁶ the Law Commission explored how social attitudes to privacy have changed over time and some of the factors that engender differing views on privacy. The Commission observed that ideas about privacy are closely associated with technological and social change⁶⁷ and are shaped by culture, history and personal experience.⁶⁸ For example, individuals from different cultural backgrounds may have differing perceptions of privacy.⁶⁹
- 2.35 The Commission noted that age was a factor that was likely to influence attitudes to privacy, as people have different experiences and expectations of privacy at different ages.⁷⁰ In addition, different generations may have different attitudes towards privacy because they have grown up in different worlds: younger generations, who have grown up in the Internet era, may have a very different sense of privacy from that of older generations.⁷¹ The Commission also observed that Māori may have different attitudes to privacy than Pākehā because of their experience of being an indigenous minority who have at times suffered discrimination and unfair treatment, including from the government.⁷²
- 2.36 The Commission analysed data available in 2008 (in opinion surveys) about public attitudes to privacy in New Zealand. It noted the limitations of relying on survey data to draw firm conclusions about public attitudes.⁷³ However, it considered it was reasonable to infer from the available data that “a majority of New Zealanders express concern about privacy, and a desire to keep their personal information private”, and that there is a much higher level of concern about some issues (for example, Internet security) than others (for example, drug testing).⁷⁴
- 2.37 We note that the results of several more recent surveys on attitudes to privacy in New Zealand suggest that public concern about privacy remains high:

64 Te Hunga Rōia also made a broader submission that the Act should include a reference to the Treaty of Waitangi. We address that point in Chapter 4 at paragraphs [4.69]–[4.84].

65 From our review of the Act, this will not result in any substantive changes to the provisions in which the phrase “private premises” appears (see ss 46–47 and 172 of the Search and Surveillance Act 2012).

66 Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008) ch 5.

67 At [5.14].

68 At [5.1].

69 See, for example, Rafael Capurro “Privacy: An Intercultural Perspective” (2005) 7 *Ethics and Information Technology* 37; Philip Brey “Is Information Ethics Culturally Relative?” in Ephrem Eyob *Social Implications of Data Mining and Information Privacy* (IGI Global, Pennsylvania, 2009) 1; and Keynote Address by Privacy Commissioner John Edwards (presented to Asian Privacy Scholars Network, 13 December 2016).

70 Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008) at [5.33].

71 At [5.34]. See also Valerie Steeves “If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective” (2008) *Canadian Journal of Criminology and Criminal Justice* 331 at 339.

72 Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008) at [5.32].

73 At [5.49]–[5.51].

74 At [5.61]. For a recent study into public attitudes towards different types of surveillance, see Milton Heumann and others “Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace” (2016) 14 *Rutgers Journal of Law and Public Policy* 37.

- A survey of attitudes to privacy in New Zealand was commissioned by the Office of the Privacy Commissioner and conducted in 2016.⁷⁵ The survey found that 65 per cent of respondents were concerned about individual privacy (around the same as in the last survey in 2014). Only 14 per cent said that they were not concerned (around the same as in 2014).⁷⁶
 - In 2015, a survey commissioned by the World Internet Project New Zealand found that a majority of respondents (68 per cent) were actively trying to protect their online privacy.⁷⁷ 29 per cent of respondents indicated they were concerned about violations of their online privacy by the government, and 42 per cent indicated they were concerned about such violations by corporate entities.
 - Another survey of New Zealanders' thoughts and attitudes towards the Internet was commissioned in 2016 by InternetNZ.⁷⁸ 94 per cent of respondents said they check the Internet at least once a day. The biggest concern about the Internet identified by respondents was the threat to the security of personal data (followed by threats to privacy, the risk of identity theft and online crime). Overall, however, attitudes towards the Internet were predominantly positive, with 89 per cent of respondents being of the view that the positives of using the Internet outweighed the negatives.
- 2.38 A number of commentators have written about the impact of advancements in new technology on societal attitudes and international trends relating to privacy.⁷⁹ It has been suggested that “[r]emarkable, and fast-moving, advances in technology have created a concern that details of our lives are able to be made available to others without consent”.⁸⁰ For example, as individuals continue to embed communication technologies into their home, places of work and so on, the amount of transactional data that is generated (often without the user being aware that this is happening) grows exponentially.⁸¹ This in turn poses a threat to the ability of individuals to control the disclosure and use of their personal information.⁸² A similar threat exists in relation

75 UMR Research *Privacy Concerns and Sharing Data* (March/April 2016) available at < www.privacy.org.nz > .

76 One part of the survey asked respondents about their attitudes to personal information being shared between organisations (both government agencies and private companies). A majority (62 per cent) felt that “we should not share data as the risks to people’s privacy outweighs the benefits”, while 38 per cent had a view closer to “we should share all the data we can because it benefits the services and me”. Respondents were more open to data sharing when safeguards were put in place: a majority were willing to share data as long as they could opt out if they chose (57 per cent), there were strict controls on who can access the data and how it is used (59 per cent) and data is anonymised and they cannot be identified (61 per cent).

77 World Internet Project New Zealand *The Internet in New Zealand* (2015) available at < www.wipnz.aut.ac.nz > .

78 UMR Research *Consumer Perceptions of the Internet* (July 2016) available at < <https://internetnz.nz> > .

79 See, for example, Brett Mason *Privacy without Principle: The Use and Abuse of Privacy in Australian Law and Public Policy* (Australian Scholarly Publishing, Melbourne, 2006) at 1, who suggests there has been increasing debate around the role of privacy in society, and that this is attributable to the impact of “intrusive new technology, heightened law enforcement powers, the promiscuous exchange of electronic data and the increasing role of surveillance in our daily lives”. Mason suggests the boundary between public and private activity has become increasingly blurred and may no longer be sustainable: at 3. See also Doyle and Bagaric, above n 24, at 168.

80 Todd, above n 25, at [17.8]. See also David Harvey “Privacy and New Technologies” in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) at [14.4].

81 Steeves “If the Supreme Court Were on Facebook”, above n 71, at 337. See also Doyle and Bagaric, above n 24, at 168 and Steven Friedland “Privacy and Democracy in the Digital Age” (2015) 20 *Media and Arts Law Rev* 1 at 10.

82 Doyle and Bagaric, above n 24, at 168. See also Privacy Commissioner *Submission to the Independent Review of Intelligence and Security by the Privacy Commissioner* (14 August 2015) at [2.4.8] and Hon Justice Michael Kirby “Privacy in Cyberspace” (1998) 21 *University of New South Wales Law Journal* 323 at 325–326: “[T]he quantity of personal information about individuals is likely to increase rather than decrease. Access to this information is what occasions the contemporary fragility of privacy ... To the extent that the individual has no control over, and perhaps no knowledge about, the mass of identifiable data which may be accumulated concerning him or her, and to the extent that national law-makers, despite their best endeavours, enjoy only limited power effectively to protect the individual in the global web, privacy as a human right, is steadily undermined”.

to user-created content, as the sharing of personal information online has become increasingly normalised.⁸³

- 2.39 The technologies of surveillance have also developed apace, allowing surveillance to be used in a growing number of contexts and prompting public debate around the role of privacy in society.⁸⁴ For example, technological developments have made the collection of “metadata” (data about data)⁸⁵ more possible than ever.⁸⁶ Kathleen Kuehn observes that:⁸⁷

‘Data about data’ provide a wealth of sensitive information potentially capable of painting a much richer picture of a person’s daily life than content alone. It is quantifiable, clean and precise; it can be organised, analysed and mapped in ways that unstructured conversations cannot be. It becomes even more valuable when aggregated and cross-referenced or ‘assembled’ with other discrete flows – for example, bank transactions, shopping purchases ..., IP addresses ..., and all of the information we give away through our web browsing behaviour, social networking and other digital interactions.

- 2.40 Donna-Maree Cross suggests that renewed public interest in privacy issues has also been driven by significant national events, including the following:⁸⁸

- The New Zealand Police’s investigation into alleged paramilitary training camps operating in the Urewera Ranges, which culminated in a series of arrests in October 2007. Police obtained a number of search warrants during the course of the investigation that sought, amongst other things, the authorisation of covert video surveillance. The lawfulness and reasonableness of the search and surveillance activities was successfully challenged in *Hamed v R*.⁸⁹ The Supreme Court unanimously held that the law at that time (prior to the Search and Surveillance Act 2012) did not permit the issuing of prospective or anticipatory warrants, so video surveillance could not be authorised.⁹⁰ In response, the Government urgently enacted legislation that allowed (with retrospective effect) the use of covert video surveillance.⁹¹ The passage of the legislation was controversial,⁹² with almost all public submissions received by the Select Committee opposed to its introduction.
- Events relating to Kim Dotcom, who the United States has been seeking to extradite (amongst other individuals) since 2012 to face trial on charges of racketeering, copyright

83 See Meredith Karlsen “Forget Me, Forget Me Not: A ‘Right to be Forgotten’ in New Zealand’s Information Society?” (2016) 3 NZ L Rev 507 at 515. Karlsen examines the implications of a decision of the European Court of Justice in Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos* [2014] ECR I-317, where the Court recognised a “right to be forgotten” on the Internet, allowing European Internet users to demand the deletion of personal information from search engine results in certain situations. See also Timothy Garton Ash *Free Speech: Ten Principles for a Connected World* (Atlantic Books, London, 2016) at 304–310. See also the discussion of “privacy as anonymity” in *R v Spencer* 2014 SCC 43, [2014] 2 SCR 212 at [38]–[49], where the Court suggested that some degree of anonymity is a feature of much Internet activity and that, depending on the totality of the circumstances, anonymity may enjoy constitutional protection against unreasonable search and seizure. See also Chris Hunt and Micah Rankin “*R v Spencer*: Anonymity, the Rule of Law, and the Shrivelling of the Biographical Core” (2015) 61 McGill LJ 193.

84 See Kathleen Kuehn *The Post-Snowden Era: Mass Surveillance and Privacy in New Zealand* (Bridget Williams Books, Wellington, 2016) at 45–48; Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at [2.3]; Donna-Maree Cross “Surveillance” in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) at [6.1]; Simon Bronitt “Electronic Surveillance, Human Rights and Criminal Justice” (1997) 3 Australian Journal of Human Rights 183; and Joseph Cannataci *Report of the Special Rapporteur on the Right to Privacy A/HRC/34/60* (2017).

85 Metadata 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 Internet Protocol (IP) addresses the communication was sent and received from. It does not include the content of communications, such as the body of an email.

86 Kuehn, above n 84, at 11.

87 At 66.

88 Cross “Surveillance”, above n 84, at [6.1].

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

90 At [6], [145]–[150] and [210]–[213].

91 Video Camera Surveillance (Temporary Measures) Act 2011.

92 Cross “Surveillance”, above n 84, at [6.4.1]; Samuel Beswick “Privacy: rights, remedies and reform” [2015] NZLJ 166 at 166; and Samuel Beswick and William Fotherby “Surveilling the stopgap” [2011] NZLJ 404 at 405.

infringement and money laundering.⁹³ An internal government investigation found that the Government Communications Security Bureau (GCSB) had unlawfully intercepted the communications of Mr Dotcom and an associate.⁹⁴ This prompted an independent review of GCSB, which found that there were 88 other instances where illegal surveillance may have occurred.⁹⁵ In response, the Government immediately introduced an amendment Bill that clarified the powers of GCSB.⁹⁶ The Bill, which was passed, was controversial. A number of public submissions were opposed to its introduction, and protests occurred throughout the country.⁹⁷

- The leaking of classified information from the United States National Security Agency in 2013 by whistle-blower Edward Snowden, which revealed details about the United States and United Kingdom surveillance programmes. In 2015, a number of leaks relating to New Zealand became public, prompting public debate over the nature and scale of global surveillance programmes and New Zealand's role in international intelligence-gathering.⁹⁸

- 2.41 A further incident that gained international scrutiny was the use of a breath-testing checkpoint by Police for non-road safety purposes to obtain the names and addresses of elderly people who had attended an Exit International (a pro-euthanasia organisation) meeting.⁹⁹ The checkpoint was set up as part of a police investigation into alleged instances of assisting suicide (an offence under the Crimes Act 1961). Police has asked the Independent Police Conduct Authority to review the incident.¹⁰⁰
- 2.42 On the other hand, terrorist attacks around the world since the enactment of the Search and Surveillance Act, along with growing concern about the Islamic State of Iraq and the Levant (ISIS), have focused increased attention on whether adequate and effective tools are available to law enforcement agencies and the intelligence community¹⁰¹ to investigate and prevent threats to national and international security.¹⁰²
- 2.43 The above discussion illustrates that there is a relatively high degree of public interest in privacy issues in New Zealand. In that context, we have been particularly mindful of privacy in conducting our review.

93 Mr Dotcom and his associates challenged the validity of search warrants issued under the Mutual Assistance in Criminal Matters Act 1992. The warrants were held to be invalid in the High Court (*Dotcom v Attorney-General* [2012] NZHC 1494, [2012] 3 NZLR 115), but the Court of Appeal subsequently overturned that decision and concluded the warrants were valid (*Attorney-General v Dotcom* [2014] NZCA 19, [2014] 2 NZLR 629). The Court of Appeal's decision was upheld by a majority of the Supreme Court in *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745.

94 Mr Dotcom was a New Zealand permanent resident. At the time, it was illegal for the Government Communications Security Bureau to conduct surveillance on New Zealand citizens or permanent residents.

95 Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013).

96 The Government Communications Security Bureau and Related Legislation Amendment Bill 2013.

97 Kuehn, above n 84, at 75.

98 See Nicky Hager and Ryan Gallagher "Snowden revelations/The price of the Five Eyes club: Mass spying on friendly nations" *The New Zealand Herald* (online ed, Auckland, 5 March 2015) and Kuehn, above n 84.

99 See Eleanor Ainge Roy "New Zealand police set up roadblocks to question euthanasia group" *The Guardian* (online ed, London, 25 October 2016).

100 See Isaac Davison "False checkpoint targeting euthanasia supports part of investigation, police confirm" *The New Zealand Herald* (online ed, Auckland, 27 October 2016).

101 As we have noted earlier in this Report, New Zealand's intelligence agencies are tasked with contributing to the protection of New Zealand's national security (including against terrorist attacks). Their objectives do not include law enforcement.

102 See the discussion in Berkman Center for Internet and Society *Don't Panic: Making Progress on the "Going Dark" Debate* (Harvard University, 1 February 2016) at 2.

RECOMMENDATION

- R2 The reference to marae in the definition of “private premises” in section 3 of the Act should be removed, and subsequent references to “private premises” in the Act should be changed to “private premises and marae”. Those references are in sections 46 (activities for which a surveillance device warrant is required), 47 (some activities that do not require a surveillance device warrant), 172 (information to be included in a report on surveillance device warrants and declaratory orders) and the Schedule (powers in other enactments to which all or part of Part 4 of the Act applies).

EFFECTIVENESS

- 2.44 This section explores what is meant by effective law enforcement. We do so by considering case law and examples in the Search and Surveillance Act. We also look at some of the current challenges to effective law enforcement.
- 2.45 Effectiveness is a central law enforcement value. This is made clear in the Policing Act 2008, which confirms that law enforcement is a key function of Police,¹⁰³ and provides that one of the principles underpinning the Act is that “principled, effective, and efficient policing services are a cornerstone of a free and democratic society under the rule of law”.¹⁰⁴
- 2.46 The reference in section 8 to the rule of law in a free and democratic society “plainly invokes”¹⁰⁵ the language of section 5 of NZBORA, which provides that “the rights and freedoms contained in this Bill of Rights may be subject to such reasonable limits prescribed by law as can be demonstrably justified in a free a democratic society”.¹⁰⁶
- 2.47 In *R v Jefferies*,¹⁰⁷ Thomas J (in one of five separate judgments) described the framework for balancing human rights values against law enforcement values when considering whether there has been an unreasonable search or seizure under section 21. What is required, he said, is an assessment as to “whether, in the particular situation, the public interest in being left alone by government must give way to the government’s interest in intruding on the individual’s privacy in order to advance its goals, notably those of law enforcement”.¹⁰⁸ His Honour also observed that law enforcement goals were not exclusively those of the government; rather, they were interests and goals of the community at large.¹⁰⁹

103 Policing Act 2008, s 9(c).

104 Policing Act 2008, s 8(a). “Policing” is defined in s 4 of the Policing Act 2008 as the performance by Police of any of its functions, which includes law enforcement (s 9(c)).

105 *K v R* [2017] NZCA 51 at [21].

106 In the search and surveillance context, the assessment of reasonableness required by section 5 is already incorporated into the test for whether there has been an unreasonable search or seizure. In other words, if there has been a breach of s 21, it is unnecessary to carry out a further analysis under s 5. See *Cropp v Judicial Committee* [2008] NZSC 46, [2008] 3 NZLR 774 at [33] and *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [162] per Blanchard J. For criticism of this approach, see Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis, Wellington, 2015) at [18.24].

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

108 At 319 per Thomas J, referring to *Hunter v Southam Inc* [1984] 2 SCR 145 at 159–160 per Dickson J.

109 At 319 per Thomas J. See also *R v Ngan* [2007] NZSC 105, [2008] 2 NZLR 48 at [104] per McGrath J: “[a]pplication of s 21 will set the point at which privacy rights are limited to accommodate *community rights*, particularly the public interest in proper law enforcement, including the detection and prosecution of criminal behaviour” (emphasis added).

2.48 As Hardie Boys J explained in *R v Jefferies*:¹¹⁰

A commonsense approach [to section 21 of NZBORA] is called for: a sensible and practical reconciliation between personal rights, individual freedom and dignity, on the one hand, and community rights, the investigation and prevention of crime, on the other. It is a fundamental community expectation that a police officer who has sworn to discharge his [or her] duties according to law will not act in disregard of the law. Yet the police are expected to act realistically when the occasion demands. Roadblocks and vehicle searches following a serious crime such as a kidnapping are an example that readily comes to mind of actions which may not in a sense be lawful, but which cannot be other than reasonable. Equally, a slip, a minor error, a technical breach, will surely not be seen as tipping the scales against due recognition of the rights of the individual. Even if it results in the police action becoming unlawful, it is only technically so, and not of a degree such as to lead it to being unreasonable.

- 2.49 The New Zealand courts have frequently recognised that police officers are expected to act realistically when the occasion demands. For example, while the courts have recognised 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, they have emphasised the need to have regard to “the practicalities of policing”¹¹¹ in urgent situations. This includes considering whether a property can be kept under surveillance and evaluating the resources available to officers at the time they assessed whether the situation made it reasonable to invoke a warrantless power.¹¹²

Moral or social duty to assist

- 2.50 A corollary of the community’s interest in proper law enforcement is that citizens are under a “moral” or “social” duty to assist police investigations into criminal offending (although there is no legal duty to that effect).¹¹³ In *Taylor v Director of the Serious Fraud Office*, Lord Hoffmann observed that:¹¹⁴

Many people give assistance to the police and other investigatory agencies, either voluntarily or under compulsion ... They will be moved or obliged to give the information because they or the law consider that the interests of justice so require.

- 2.51 The Policing Act 2008 also expressly recognises that effective policing relies on a range of partner organisations in the public and private sectors, as well as the efforts of individuals, families and communities.¹¹⁵ Section 8 states that “effective policing relies on a wide measure of public support and confidence”,¹¹⁶ and section 10 provides:

10 Roles of others acknowledged

- (1) It is acknowledged that important and valuable roles in the performance of the functions of the Police are played by—

110 *R v Jefferies* [1994] 1 NZLR 290 (CA) at 315 per Hardie Boys J. See also *R v Dodgson* (1995) 2 HRNZ 300 (CA) at 303, where the Court of Appeal relied on this passage in determining whether an external observation of a car amounted to a “search”. The Court held that “not every such observation, in so far as it could be described as a search, attracts the need for statutory authority, or a search warrant. That would make policing intolerable” (at 303). See also *Williams v Police* [1981] 1 NZLR 108 (HC) at 113: “The police must be enabled to pursue their duty without the hindrance of an over-zealous ex post facto examination of the reasonableness of their actions”.

111 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [24] per William Young P and Glazebrook J. See also at [120].

112 At [24]. See also *R v T* [2008] NZCA 99 at [16]; *R v Dobson* [2008] NZCA 359 at [38]; and *Hughes v R* [2011] NZCA 661 at [25]. There have been a number of recent cases in the Court of Appeal where this issue has arisen in the context of searches of electronic devices: see the cases referred to in n 38 of Chapter 12.

113 See *Rice v Connolly* [1966] 2 QB 414 at 419 (“every citizen has a moral duty or, if you like, a social duty to assist the police”). See also *Moulton v Police* [1980] 1 NZLR 443 (CA) at 444.

114 *Taylor v Director of the Serious Fraud Office* [1998] UKHL 39, [1998] 3 WLR 1040 at 1049.

115 See Policing Bill 2007 (195-1) (explanatory note) at 3.

116 Policing Act 2008, s 8(b).

- (a) public agencies or bodies (for example, certain departments of State, and local authorities); and
 - (b) the holders of certain statutory officers (for example, Māori wardens); and
 - (c) parts of the private sector (for example, the private security industry).
- (2) It is also acknowledged that it is often appropriate, or necessary, for the Police to perform some of its functions in co-operation with individual citizens, or agencies or bodies other than the Police.

Examples of provisions in the Act designed to promote effectiveness

2.52 As the Law Commission observed in its 2007 Report, the concept of “effectiveness” requires search powers to be able to be effectively deployed. Where powers are granted in an overly restrictive fashion, they are likely to frustrate law enforcement officers. In turn, frustration may encourage a number of negative reactions. Some officers may ignore trivial restrictions and thereby contribute to a culture where legal regulation of search powers is regarded with contempt or disdain. Others may refrain from enforcing the law itself, since detecting and investigating a breach of it is too difficult.¹¹⁷

2.53 A number of the Commission’s 2007 recommendations (which were ultimately accepted) were specifically designed to enable effective law enforcement. For example, the Commission recommended the following:

- There should be an ability to apply for a search warrant orally where delay in making the application in writing would compromise the effectiveness of the search.¹¹⁸
- Enforcement officers exercising search powers should have the ability to secure the scene and give reasonable directions to any person at the place being searched to enable the search to be carried out effectively, or for the purpose of preserving evidence or preventing its destruction or concealment.¹¹⁹
- In exceptional circumstances, Police should have the ability to search private places and vehicles without warrant for evidential material relating to serious crimes.¹²⁰ In addition, the Commission considered a corresponding power to search a person in a public place was necessary.¹²¹

Challenges to law enforcement in the digital age

2.54 Changes to technology and the way in which people use it are placing considerable new pressures on the effective deployment of search and surveillance powers. While technological developments give law enforcement agencies new investigative techniques and strategies, they also provide new opportunities for crimes to be committed and in increasingly sophisticated ways.¹²²

117 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [2.27].

118 At [4.59] and recommendation 4.14. See now s 100(3)(a) of the Search and Surveillance Act 2012.

119 At [4.59] and recommendation 6.22. See now s 116 of the Act.

120 Recommendations 5.13 and 9.14. See now ss 15 and 17 of the Act.

121 At [8.46] and recommendation 8.12. See now s 16 of the Act.

122 Ed Cape “Search and surveillance powers” [2008] NZLJ 75 at 75.

- 2.55 The following trends have created significant challenges for the effective investigation and detection of crime, which were not as significant when the Law Commission wrote its Report in 2007:
- encryption (often automatic) of data on devices;
 - internet anonymity;
 - the increasing volume and diversity of data stored in an electronic form; and
 - the rise of cloud computing.

Encryption

- 2.56 Encryption is 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. It is a tool designed to protect the privacy and security of digital content.¹²³
- 2.57 Over the past few decades, access to encryption technology has become increasingly widespread. Encryption applies—often by default—to a range of electronic communications, such as emails and online chat services, with the effect that only the sender and recipient can read the content (known as end-to-end encryption).¹²⁴
- 2.58 With encryption widely available today, it is now possible for law enforcement agencies to have physical access to data but not be able to interpret the data without the co-operation of parties with access to the relevant decryption keys.¹²⁵ Law enforcement agencies have expressed concerns that the use of encryption by criminals is stymying investigations.¹²⁶
- 2.59 We return to the issue of encryption in Chapter 12.

Anonymity

- 2.60 Another privacy-enhancing technology that allows individuals to take control of their personal information is anonymity. Anonymity services allow users to enter and move about the Internet without leaving identifying “footprints”. Specific services include anonymous web browsing, URL encryption and anonymous re-mailers. Browsers can also be configured so that they will notify the user that a site requires cookies¹²⁷ to be accepted as a condition of access.¹²⁸
- 2.61 One of the most well-known anonymity services is Tor.¹²⁹ Tor encrypts its users’ communications then routes these communications through a network of relays located around the world.¹³⁰

123 See Joy Liddicoat “The Dark Side of the Internet” in *Cyber Law Conference* (NZLS Seminar, Auckland and Wellington, May 2016) 31 at 32–33 and Doyle and Bagaric, above n 24, at 175.

124 See Hugh McCarthy “Decoding the Encryption Debate: Why Legislating to Restrict Strong Encryption Will Not Resolve the ‘Going Dark’ Problem” (2016) *Journal of Internet Law* 17 at 18.

125 Waldo, Lin and Millett, above n 13, at 266. See also Devin Adams “The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, ‘Particularly’ Speaking” (2017) 3 *University of Richmond L Rev* 727 at 730.

126 Waldo, Lin and Millett, above n 13, at 266; McCarthy “Decoding the Encryption Debate”, above n 124, at 18. See also Hal Abelson, Ken Ledeen and Harry Lewis *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (Addison-Wesley, United States, 2008) at 161. The growing gap between the legal powers and authority of law enforcement agencies to access evidential material and their technical capacity to actually do so—due to barriers such as encryption—has been described as the “going dark” problem. This term was first used by the United States Federal Bureau of Investigation in 2010. See McCarthy “Decoding the Encryption Debate”, above n 124, at 18 and 21.

127 A “cookie” is a small text file created by a website that is stored in a user’s computer either temporarily or permanently. Cookies provide a means for websites to recognise users and track their preferences.

128 See, for example, Sara Silva and Chris Reed “You Can’t Always Get What you Want: Relative Anonymity in Cyberspace” (2015) 12 *SCRIPTed* 35; and Doyle and Bagaric, above n 24, at 175.

129 An acronym for “The Onion Router”.

130 See Arran Hunt “The Dark Side of the Internet” in *Cyber Law Conference* (NZLS Seminar, Auckland and Wellington, May 2016) 3 at 7–8.

- 2.62 Anonymity services create challenges for law enforcement agencies because they make it difficult (and sometimes impossible) to identify the individuals who have created, sent or received digital content.¹³¹ For example, in 2014, the United States Federal Bureau of Investigation (FBI) became aware of a Tor site that was hosting child exploitation material. The FBI obtained a search warrant and seized the server that was hosting the site. It then sent malware (software used to disrupt computing systems) to visitors of the site, which revealed their identities and locations.¹³² The case has prompted a number of ongoing legal challenges and has sparked wider debate about the FBI's use of hacking technology.¹³³

Increasing volume and diversity of data

- 2.63 Since the enactment of the Search and Surveillance Act, there has been an exponential growth in the storage of information in an electronic form.¹³⁴ 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.¹³⁵
- 2.64 The growth in the volume of digital data has presented opportunities for law enforcement agencies to access information about individuals that previously may not have existed in a non-digital form. However, it also presents some challenges for effective law enforcement. As criminal investigations are increasingly likely to involve digital evidence, there is a growing need for investigators to have expertise in collecting and analysing digital evidence and to have access to specialised digital forensic tools.¹³⁶ Moreover, the sheer volume of data that may need to be processed may exceed the capacity of law enforcement agencies to analyse it.¹³⁷ It has been suggested that:¹³⁸

The challenges associated with this growth are likely to become more even problematic over time, as digital data becomes more ingrained into the fabric of everyday life. These challenges will necessitate organisational, training, financial, and operational evolution if law enforcement is to provide competent and timely service in the coming years.

- 2.65 A related challenge for law enforcement agencies is the increasing diversity of storage methods for digital data, as agencies may be required to recognise new media, obtain technology to read new objects and formats and develop the expertise to forensically examine each new format.¹³⁹

Cloud computing

- 2.66 Cloud computing is a method of storing and accessing data and programs using remote servers hosted on the Internet rather than on a local server or personal computer. In 2015, a survey of 1,377 New Zealanders commissioned by the World Internet Project New Zealand found that nearly half (49 per cent) of Internet users use cloud computing.¹⁴⁰

131 Waldo, Lin and Millett. above n 13, at 266 and 268.

132 See Ellen Nakashima "This is how the government is catching people who use child porn sites" *The Washington Post* (online ed, Washington DC, 21 January 2016); and Orin Kerr "Government 'hacking' and the Playpen search warrant" *The Washington Post* (online ed, Washington DC, 27 September 2016).

133 See Nakashima, above n 132; and Kerr, above n 132. For an example of how New Zealand Police has attempted to identify individuals who have downloaded child exploitation material from Internet sites, see *Arnerich v R* [2012] NZCA 291 at [10]–[12].

134 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [6.1] and [6.3] [Issues Paper].

135 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).

136 Hossein Bidgoli *Handbook of Information Security* (Vol 2, John Wiley & Sons, United States, 2006) at 697. See also David Lillis and others "Current Challenges and Future Research Areas for Digital Forensic Investigation" (2016) CDFSL Proceedings 9.

137 Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009) at [8.36].

138 Bidgoli, above n 136, at 699.

139 At 699.

140 World Internet Project New Zealand *The Internet in New Zealand* (2015) available at < www.wipnz.aut.ac.nz > .

2.67 The use of cloud computing presents significant challenges for law enforcement agencies. Sometimes data stored in the Cloud may be distributed over different servers, providers, locations and jurisdictions.¹⁴¹ The location of that data may also be constantly changing. In practical terms, this means the location of data stored in the Cloud may sometimes be unknowable. Further, where data is stored outside of New Zealand, law enforcement agencies may face jurisdictional challenges in seizing that material. As we discussed in our Issues Paper¹⁴² and explore later in Chapter 12, there is currently a degree of uncertainty about the ability of enforcement officers to access information stored on servers in other jurisdictions. This can impede the ability of enforcement agencies to collect information in a timely fashion.

SECTION 30 OF THE EVIDENCE ACT 2006

2.68 Section 30 of the Evidence Act 2006 determines the basis on which improperly obtained evidence may be admissible in criminal proceedings. The relationship between the Search and Surveillance Act and section 30 is significant because challenges to the exercise of search or surveillance powers are frequently made by means of challenging the admissibility of evidence. As we noted earlier in this Report, our review has not been concerned with the operation of section 30 itself. That section is specifically being considered by the Law Commission in the context of its second statutory review of the Evidence Act, which commenced in February 2017.¹⁴³

2.69 Evidence obtained as a result of an unlawful or unreasonable search will be “improperly obtained” for the purposes of section 30. The route to section 30 can be either direct or indirect:¹⁴⁴

- An example of the direct route is where the preconditions for exercising a warrantless power or issuing a warrant under the Act are not properly established.¹⁴⁵ The exercise of the warrantless power or issue of the warrant would be unlawful, and any evidence obtained as a result would be improperly obtained.
- An example of the indirect route is where a warrant is lawfully issued but the manner in which it is executed is unreasonable, thus breaching section 21 of NZBORA.¹⁴⁶ Any evidence obtained as a result of such a search would be improperly obtained.

2.70 However, exclusion of the evidence is not a guaranteed result.¹⁴⁷ 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

141 Lillis and others “Current Challenges”, above n 136, at 12. See also G Grispos, T Store and W B Glisson “Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics” (2012) 4 *International Journal of Digital Crime and Forensics* 28.

142 Issues Paper, above n 134, at [6.113].

143 The Law Commission must report to the Minister of Justice by 20 February 2019.

144 See Issues Paper, above n 134, at [1.48]–[1.50].

145 For example, in *A v R* [2016] NZCA 402 a warrantless search of a vehicle under s 20 of the Search and Surveillance Act 2012 was unlawful because not all of the preconditions for exercising the power had been met.

146 For example, in *R v Pratt* [1994] 3 NZLR 21 (CA), Police had the requisite belief to invoke a warrantless power to conduct a personal search of the accused. However, the search was held to be unreasonable because he was strip-searched in a public place, when there was no reason why he could not have been searched in private.

147 Our review of cases available on *Westlaw NZ* and *LexisNexis* since the Search and Surveillance Act 2012 came into force until 26 June 2017 suggests that there have been 31 cases where searches conducted under that Act were found to be unlawful and/or unreasonable. The evidence obtained as a result of those searches was admitted under s 30 of the Evidence Act 2006 in 22 of those cases, and excluded in the remaining 9 cases. The implications of this are to be considered during the second statutory review of the Evidence Act: see paragraph [2.68].

effective and credible system of justice”.¹⁴⁸ A number of non-exhaustive factors are listed in section 30 for the judge to consider.¹⁴⁹

- 2.71 Because section 30 does not automatically result in the exclusion of improperly obtained evidence, it cannot be relied on as a way to hold enforcement officers to account for unlawful or unreasonable searches.¹⁵⁰ This is illustrated by recent Court of Appeal decisions that have expressly rejected the proposition that carelessness on the part of enforcement officers concerning their powers under the Search and Surveillance Act should be influential in favouring exclusion.¹⁵¹ For example, in *Young v R*, the Court said:¹⁵²

It seems to us that [counsel’s] submission rests on the proposition that where a police officer fails to obtain the necessary authority for a search because of an incorrect view of the law, the evidence should be inadmissible as this will create the necessary incentive for the police to get the law right. Such an approach is inconsistent with the scheme of s 30.

- 2.72 In addition, because section 30 only applies to criminal proceedings, it can only provide an avenue for challenging the legitimacy of a search where charges are laid and the case proceeds to trial.¹⁵³ This also means that section 30 can only ever provide a means of determining—after the fact—whether a search ought to have occurred (rather than preventing unlawful or unreasonable searches from occurring).¹⁵⁴ Because of this, section 30 does not proactively protect individuals’ privacy rights: it is unable to act as a preventative or “prophylactic device” against unjustified State intrusion before a search takes place.¹⁵⁵
- 2.73 One of our aims in this review is to promote a more proactive approach to protecting individuals’ rights when search and surveillance powers are exercised. We have therefore considered how the Search and Surveillance Act could be amended to ensure decisions about how and when to undertake a search or seizure are made *in advance* of their execution rather than being considered in hindsight.

LAW ENFORCEMENT AND REGULATORY POWERS

- 2.74 The purpose of this discussion is to highlight the different considerations that apply when considering the extent to which powers of search and seizure ought to be conferred on law enforcement and regulatory agencies. As we go on to suggest at paragraph [2.84] below, this is a significant issue that we consider requires further research and analysis by the Ministry of Justice.

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

149 Evidence Act 2006, s 30(3). The leading case on the application of s 30 to search and surveillance activity is *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 (to be read together with *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729).

150 That is not to say that s 30 cases never contribute to the development of improved procedures and better training for enforcement officers. For example, Elisabeth McDonald observes that “expecting police to operate within the law during an investigative process is an important aspect of a legitimate system of justice and exclusion of evidence is a very real (and significant) reminder of this expectation”: *Principles of Evidence in Criminal Cases* (Thomson Reuters, Wellington, 2012) at 246.

151 See *Young v R* [2016] NZCA 107 at [23]–[25], *K v R* [2016] NZCA 259 at [30] and *R v R* [2016] NZCA 200 at [31].

152 *Young v R* [2016] NZCA 107 at [25]. In contrast, earlier (pre-Evidence Act 2006) decisions of the Court of Appeal suggested the court was willing to exercise “its general supervisory and disciplinary responsibilities” and exclude evidence to “emphasise the need for the police to comply with the requirements of the statutes under which they exercise their powers”: *R v Mann* [1991] 1 NZLR 458 (CA) at 465; *R v Convery* [1968] NZLR 426 (CA) and *R v Hartley* [1978] 2 NZLR 199 (CA). See also the discussion in Richard Mahoney “Evidence” (1992) NZ Recent L Rev 29 at 40–43 and Richard Mahoney “Vindicating Rights: Excluding Evidence Obtained in Violation of the Bill of Rights” in Grant Huscroft and Paul Rishworth (eds) *Rights and Freedoms* (Brookers Ltd, Wellington, 1995) 447.

153 Furthermore, “[i]t depends upon the defence (whose role is to represent the accused, not to regulate investigation) raising an appropriate challenge, which is itself dependent upon the defence having sufficient information to realise that a challenge is there to be raised”: Clive Harfield “The Governance of Covert Investigation” (2010) 34 Melbourne University L Rev 773 at 780.

154 See Harfield “The Governance of Covert Investigation”, above n 153, at 781, who suggests that the laws of evidence cannot “effectively and consistently achieve regulation of investigation—even if they can certainly influence such regulation—because their strictures are applied at the discretion of the judge, many weeks (if not months or years) after the conduct that needed to be controlled”.

155 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [263] per Hammond J.

2.75 This issue is explored in some detail in *The New Zealand Bill of Rights Act: A Commentary*.¹⁵⁶ The authors begin their discussion by outlining the distinction between offences in regulatory statutes (sometimes called “public welfare regulatory offences”¹⁵⁷) and criminal statutes (“true crime offences”). They explain that the distinguishing characteristics relate to the nature of the conduct addressed by the legislation, and the purpose for which the legislation is designed:¹⁵⁸

As regards the first, criminal offences are usually concerned with conduct which by its very nature is morally reprehensible. By contrast regulatory offences are part of an overall scheme designed to secure compliance with statutorily determined standards of care. Regulatory offences are generally created for instrumental reasons connected with the need to provide a scheme of effective inducements to compliance. Thus, consideration of the “stigma” attaching to an offence will be a significant clue as to the nature of the conduct at issue.

As regards the second, much regulatory legislation is designed to prevent the occurrence of harm to members of society. It does this by information-gathering processes, monitoring, and setting standards in light of developments in science and industry. The aim of regulatory offences is to ensure compliance with those standards. Criminal law, by contrast, is aimed at underlining important social values. Thus, consideration of the purpose of the statute is another clue as to its classification.

2.76 The authors go on to observe that regulatory agencies have traditionally enjoyed very broad types of search and seizure powers and have not been subjected to standards as exacting as those applicable to criminal investigations.¹⁵⁹ For example, a number of regulatory statutes permit searches and/or seizure in the absence of a warrant. Examples include on-the-spot inspections of persons, premises and vehicles involved in closely regulated industries such as fisheries,¹⁶⁰ agriculture,¹⁶¹ and health and safety.¹⁶² Furthermore, a number of search and seizure powers in the regulatory context do not depend on the existence of a threshold before they are exercised.¹⁶³

2.77 Regulatory powers of search and seizure are often wider than law enforcement powers because:¹⁶⁴

- it is essential for regulatory agencies to be able to effectively conduct investigations in order to deter non-compliance;
- the information that leads to proof of non-compliance often lies exclusively in the control and knowledge of the person being regulated; and
- regulatory offending is less likely to have a direct victim, making it harder to detect cases of non-compliance.

2.78 Because of the unique context in which these powers are exercised, it is arguable that industry participants have a lesser expectation of privacy in the regulatory environment. They may

156 Butler and Butler, above n 106, at [18.29]. See also Andrew Butler “Regulatory Offences and the Bill of Rights” in Grant Huscroft and Paul Rishworth (eds) *Rights and Freedoms* (Brookers Ltd, Wellington, 1995) 347.

157 A P Simester and W J Brookbanks *Principles of Criminal Law* (4th ed, Brookers Ltd, Wellington, 2012) at 139. These offences fall into two categories: strict liability and absolute liability.

158 Butler and Butler, above n 106, at [18.29.2]. See also *Cross on Evidence* (online ed, LexisNexis, Wellington) at [2.3.1(d)], where it is noted that, although there is “no hard and fast rule” for distinguishing between the two types of offences, considerations can be distilled from case law (*Millar v Ministry of Transport* [1986] 1 NZLR 660 (CA) and *AHI Operations Ltd v Department of Labour* [1986] 1 NZLR 645 (HC)): whether the offence regulates a trade or activity; whether alternative truly criminal charges are available if damage or injury results; whether it is unreasonable to require the prosecutor to prove the detail of what occurred; whether the sentence is appropriate to a welfare offence; and whether the offence carries any social stigma. See also *Comité Paritaire de l’Industrie de la Chemise v Potash* (1994) 115 DLR (4th) 702 at 713 and *Law Commission Entry, Search and Seizure* (NZLC PP50, 2002) at 3–4.

159 Butler and Butler, above n 106, at [18.29.4].

160 For example, s 199 of the Fisheries Act 1996.

161 For example, s 87 of the Animal Products Act 1999.

162 For example, s 168 of the Health and Safety at Work Act 2015.

163 For example, s 87(1) of the Animal Products Act 1999.

164 Butler and Butler, above n 106, at [18.29.4]. See also Butler “Regulatory Offences and the Bill of Rights”, above n 156, at 350–351.

expect that—as part of doing business—their activities will be subject to inspection and examination.¹⁶⁵

- 2.79 This does not mean, however, that regulatory powers are not subject to section 21 of NZBORA. The courts have confirmed the relevance of section 21 to such powers on a number of occasions.¹⁶⁶ When assessing the reasonableness of regulatory powers, the authors of *The New Zealand Bill of Rights Act: A Commentary* suggest that a number of factors are relevant, including: the nature of the particular activity that is subject to regulation; the extent to which privacy can be reasonably expected in the circumstances; the type of intrusion involved; the need for unannounced inspection conducted on a random basis; and the utility or practicality of a warrant regime in the circumstances.¹⁶⁷ They observe that, although limitations on reasonable expectations of privacy may be easier to justify in many regulatory contexts,¹⁶⁸ this does not obviate the need to conduct a detailed assessment of the balance to be struck between regulatory concerns and the privacy interests at stake.¹⁶⁹

Regulatory powers and the Search and Surveillance Act

- 2.80 It is clear from the discussion above that the particular nature of regulatory compliance regimes gives rise to different issues than those experienced in the law enforcement environment.
- 2.81 In our Issues Paper, we explained how the Law Commission’s 2007 Report only considered search and seizure in the context of law enforcement.¹⁷⁰ It did not address search or inspection powers in a regulatory context.¹⁷¹
- 2.82 After the 2007 Report was published, a decision was made to extend the operation of aspects of Part 4 of the Act (which sets out general provisions in relation to the exercise of search, surveillance and inspection powers) to apply to some powers exercised for regulatory compliance purposes as well.¹⁷² (Those powers themselves are located in the relevant regulatory agency’s empowering legislation.¹⁷³) 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. The powers contained in Part 3 of the Act (which confers the ability to apply for surveillance device warrants, declaratory orders and production orders) are also available to “enforcement officers”, which includes not only police officers but also other officers who have specified powers of entry, search, inspection, examination or seizure.¹⁷⁴

165 Butler and Butler, above n 106, at [18.24.20] and [18.29.5].

166 See *TranzRail v Commerce Commission* [2002] 3 NZLR 780 (CA); *Tauber v Commissioner of Inland Revenue* [2012] NZCA 411, [2012] 3 NZLR 549; and *Henderson v Attorney-General* [2017] NZHC 606.

167 Butler and Butler, above n 106, at [18.25.19].

168 At [18.29.5]. The authors refer to jurisprudence in Canada and the United States (at [18.29.6]–[18.29.31]), which “shows broad support for greater intrusion on privacy and reduced expectations of privacy in the regulatory environment” (at [18.29.6]). See, for example, *Thomson Newspapers Ltd v Canada* [1990] 1 SCR 425 at [121]–[122] per LaForest J.

169 At [18.29.31].

170 Issues Paper, above n 134, at [1.53]–[1.56].

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

172 See the discussion in Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [374]–[389].

173 See the discussion in Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [62]–[64].

174 See the definition of “enforcement officer” in s 3 of the Act: “(a) a constable; or (b) any person authorised by an enactment specified in column 2 of the 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”.

- 2.83 While writing this Report, we came across several instances where the application of the Act to the exercise of powers in both enforcement and regulatory contexts had created “a less than comfortable operational fit”.¹⁷⁵ For example:
- parts of the Act are premised on the ability to obtain a search warrant,¹⁷⁶ whereas some regulatory agencies have extensive warrantless powers of search or inspection and can only obtain warrants in limited circumstances;¹⁷⁷ and
 - the inclusion of regulatory powers in the Schedule has also resulted in broadening regulatory powers in some areas (for example, by allowing regulatory agencies with inspection powers to search electronic devices under section 110 of the Act).
- 2.84 We consider that the difficulty in accommodating both law enforcement and regulatory powers in one Act will only continue as further amendments to the Act are contemplated. For that reason, we see value in a separate stream of work being conducted by the Ministry of Justice. This could examine how the two types of powers differ and the extent to which the Act can appropriately be applied to regulatory agencies. For example, such a review could consider:
- the extent to which the principles we identify in Chapter 4 are applicable to the powers listed in the Act’s Schedule, to which Part 4 of the Act applies;¹⁷⁸
 - the extent to which surveillance device warrants and production orders under the Act should be available to enforcement officers exercising warrantless powers listed in the Act’s Schedule;
 - the extent to which the covert operations regime we propose in Chapter 15 should apply to non-Police agencies;
 - the extent to which the warrant preference approach for searches of electronic devices, which we propose in Chapter 12, can and should apply to the regulatory powers listed in the Act’s Schedule; and
 - whether, as a result, any required amendments are best placed within the Act or the legislation that confers the regulatory power.

THE CONCEPT OF INFORMED CONSENT

- 2.85 There is a final point that we highlight here. We refer to the concept of consent in a number of different places in this Report. For example, in Chapter 9, we recommend that the Act should be amended so that a surveillance warrant is not required to track a person with their consent or to track a thing with the consent of the person entitled to possession of it. In that chapter we also consider whether the Act should continue to permit oral communications to be covertly recorded without a warrant if at least one party to the communication consents. In Chapter 17, we recommend that the Act be amended to accommodate out-of-court procedures for resolving privilege claims, provided the privilege holder consents to the alternative procedure.

175 Issues Paper, above n 134, at [1.56].

176 Search and Surveillance Act 2012, ss 51(a)(i) (surveillance device warrants) and 71(1) (production orders).

177 For example, park rangers have warrantless powers to enter vehicles and structures in national parks for evidence of offending but cannot apply for a warrant to do so: s 65(1) of the National Parks Act 1980.

178 For example, we envisage that it may be unrealistic for the proportionality principle we recommend in Chapter 4 to apply to the exercise of regulatory inspection powers; however, it may well be appropriate in respect of most threshold-based powers.

- 2.86 Consent is not a novel concept in the Act. There are a number of provisions in the Act that refer to the concept of consent,¹⁷⁹ which often features as an exception from rules that would otherwise apply. The Act is silent as to what amounts to valid consent for the purposes of those provisions, except (to an extent) in relation to “consent searches”. The provisions in subpart 2 of Part 4 set out the purpose for which a consent search may be conducted¹⁸⁰ and establish preconditions for a valid consent.¹⁸¹ Where the Act is silent, the requirements for an “informed and true consent”¹⁸² are to be found in case law.¹⁸³ It is evident from the case law that whether effective consent was provided in any given case is a question of fact and degree and is highly dependent upon all the surrounding circumstances.¹⁸⁴
- 2.87 During our consultation process, no significant concerns were raised about the absence of comprehensive preconditions for establishing valid consent in the Act. While some issues about consent searches were raised, these are relatively discrete and have been placed on the register of issues for the Ministry of Justice to consider during any subsequent reform process. This Report does not recommend reform of the general rules relating to consent.

179 See, for example, ss 47(1)(b), 91–96, 124(1), 140(5)(a) and 160(2)(a)(i) of the Search and Surveillance Act 2012.

180 Search and Surveillance Act 2012, s 92.

181 Before conducting a search by consent, the enforcement officer must advise the person from whom consent is sought of the reason for the proposed search; and must advise the person that they may either consent to the search or refuse to consent to the search (s 93). The person must have authority to give consent (s 94(c)). Section 95 expressly states that a person under the age of 14 years is unable to consent to the search of a place, vehicle, or other thing.

182 *R v Rodgers* CA65/06, 29 May 2006 at [19].

183 See the principles set out in *Wanoa v R* [2010] NZCA 33 at [25]–[28]. The Court referred to *R v Rodgers* CA65/06, 29 May 2006 at [21], where the Court of Appeal said that “an informed and true consent” must possess the following attributes: “the consent should be both informed, in the sense that the person giving it understands what it is they are being asked to consent to, and that they understand they have a choice whether to consent or not and also a true, or free, consent in the sense that the person giving the consent does not have their will overborne”. The Court in *Wanoa* also referred to *R v Gebremichael* CA19/06, 6 July 2006 and *R v Hjelmstrom* (2003) 20 CRNZ 208 (CA) at [13].

184 As the Court of Appeal described it in *Wanoa v R* [2010] NZCA 33 at [28], “[e]verything, of course, depends on the case”. See, for example, *White v Police* [2015] NZHC 1547, *Collett v Police* [2014] NZHC 3077 and *R v Su* HC Auckland CRI-2006-092-16424, 10 July 2008.

Chapter 3

The case for a principles provision

INTRODUCTION

- 3.1 In this chapter and in Chapter 4, we outline one of our key recommendations, that the Search and Surveillance Act 2012 (the Act) be amended to include a “principles” provision.
- 3.2 In this chapter, we discuss principles provisions in general, and set out their value and functions. We then explain why we think the Act would benefit from having a principles provision and how we envisage that provision would operate in practice.
- 3.3 In Chapter 4, we set out the principles that we recommend should be included in the provision and our reasons for selecting them. We note here that the principles we recommend are primarily based on existing case law. They are not intended to create any new legal obligations but are instead intended to reflect best practice as to when and how search powers are exercised under the Act. Our goal is to promote greater clarity and transparency in relation to these decision-making processes whilst also retaining the flexibility required for effective law enforcement.

THE VALUE AND FUNCTIONS OF PRINCIPLES PROVISIONS

- 3.4 Broadly speaking, a purpose provision explains why the law is being enacted,¹ while a principles provision sets out a statement of the principles that those who exercise powers under the Act are required to take into account.²
- 3.5 In the past two decades, there has been an increasing trend of incorporating purpose and principles provisions in legislation.³ This trend is partly attributable to the movement towards using “plain language” in statutory drafting⁴ as well as the increasing emphasis that has been placed on the purposive approach to statutory interpretation in recent years.⁵

1 Law Commission *Legislation Manual: Structure and Style* (NZLC R34, 1996) at [39].

2 Ross Carter *Burrows and Carter Statute Law in New Zealand* (5th ed, online ed, LexisNexis, Wellington, 2015) at 138 [Burrows and Carter]. We note that principles provisions tend to be viewed by academic commentators as a particular type of purpose provision. For that reason, there is little commentary discussing the specific use of principles provisions—as distinct from purpose provisions—in legislation. For example, the *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) do not say anything about them.

3 See *Burrows and Carter*, above n 2, at 138–139.

4 For a general history of the movement towards plain language in legislation, see *Burrows and Carter*, above n 2, ch 4. From 1987–1996, the Law Commission published a series of reports advising on ways in which the law could be made as accessible as possible. In those reports, the Commission promoted the use of purpose provisions: see Law Commission *A New Interpretation Act: To Avoid “Prolivity and Tautology”* (NZLC R17, 1990) at [229]; Law Commission *The Format of Legislation* (NZLC R27, 1993) at 9–10; and Law Commission *Legislation Manual: Structure and Style* (NZLC R34, 1996) at [30].

5 John Burrows “The Interpretation Act 1999” in Rick Bigwood (ed) *The Statute: Making and Meaning* (LexisNexis, Wellington, 2004) 211 at 220. Although there has been a legislative direction in New Zealand for over a century that the purposive approach to interpretation should be used (see now s 5(1) of the Interpretation Act 1999), it is only in the last few decades that the New Zealand courts have given the purposive approach a dominant place in statutory interpretation: see *Burrows and Carter*, above n 2, at 225. The readiness of the courts to adopt a purposive approach to statutory interpretation “increases the need for drafters to make the purpose of legislation clear in the legislation itself”: Helen Xanthaki *Thornton’s Legislative Drafting* (5th ed, Bloomsbury Professional Ltd, United Kingdom, 2013) at [8.28].

- 3.6 The Law Commission has contributed to this trend by recommending the inclusion of purpose and principles provisions on a number of occasions: for example, in its draft Evidence Code in 1999;⁶ during its review of the sanctions and remedies associated with harmful digital communications;⁷ and most recently in its draft Administration of Justice (Reform of Contempt of Court) Bill.⁸
- 3.7 The courts in New Zealand have rarely commented on the utility of purpose and principles provisions, but to the extent they have, they appear to find them helpful.⁹ Commentary also suggests that several useful functions can be performed by incorporating purpose and principles provisions in legislation:¹⁰
- they can promote accessibility and transparency in the law, by clarifying to the reader what the legislation is seeking to achieve;¹¹
 - they can guide the interpretation of the Act, both for its users and for the courts when they are required to apply the law;¹² and
 - they can constrain the exercise of legislative and administrative decision-making by indicating the factors that must be considered and/or balanced when exercising powers under the Act.¹³
- 3.8 For example, the purpose and principles provisions of the Sentencing Act 2002¹⁴ were intended to codify well-established sentencing principles in order to provide greater clarity to both the courts and the public about the sentencing process.¹⁵ They therefore perform an accessibility and transparency function.

6 See Part 2 of the draft Evidence Code in Law Commission *Evidence: Evidence Code and Commentary* (NZLC R55 Vol 2, 1999); and now ss 6–8 of the Evidence Act 2006.

7 See now s 6 of the Harmful Digital Communications Act 2015, which sets out ten “communication principles”. The Commission recommended the inclusion of these principles to “make accessible to ordinary citizens the fundamental legal rights and responsibilities which attach to the use of modern communication technologies”: Law Commission *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (Summary of Ministerial Briefing Paper, 2012) at [60(c)].

8 See cl 3 (“purposes and objectives”) of the draft Administration of Justice (Reform of Contempt of Court) Bill in Law Commission *Reforming the Law of Contempt of Court: A Modern Statute* (NZLC R140, 2017) at 147.

9 See, for example, *B v K* [2010] NZCA 96, [2010] NZFLR 865 at [49]–[52]; *Hessell v R* [2010] NZSC 135, [2011] 1 NZLR 607 at [42]–[43]; and *Ashburton Acclimatisation Society v Federated Farmers of New Zealand Inc* [1988] 1 NZLR 78 (CA) at 88 per Cooke P. See also *M v B* [2006] 3 NZLR 660 (CA) at [221] per Hammond J and *Clayton v Clayton* [2016] NZSC 29, [2016] 1 NZLR 551 at [16] and [38].

10 We note there is little empirical evidence on the operation of purpose and principles provisions. See Jeffrey Barnes “Statutory Objects Provisions: How Cogent is the Research and Commentary?” (2012) 34 *Statute L Rev* 12.

11 *Burrows and Carter*, above n 2, at 123; Duncan Berry “Purpose Sections: Why they are a Good Idea for Drafters and Users” (2011) *Loophole* 49 at 61; and Sir William Dale “Principles, Purposes and Rules” (1988) *Statute LR* 15 at 24.

12 Berry “Purpose Sections”, above n 11, at 50; Dale “Principles, Purposes and Rules”, above n 11, at 24; *Halsbury’s Laws of Canada* (online looseleaf ed, LexisNexis) at [HLG-16]; and *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) at 46.

13 *Burrows and Carter*, above n 2, at 123; Berry “Purpose Sections”, above n 11, at 51; *Halsbury’s Laws of Canada* (online looseleaf ed, LexisNexis) at [HLG-16].

14 Section 7 of the Sentencing Act 2002 codifies the purposes for which a sentence may be imposed. It consists of functional justifications for imposing a legal sanction or punishment on an offender. Section 8 then sets out a non-exhaustive list of principles of sentencing that must be applied in every sentencing decision.

15 See the Sentencing and Parole Reform Bill 2002 (148-2) (select committee report) at 1 and 6. See also *Hessell v R* [2010] NZSC 135, [2011] 1 NZLR 607 at [42]–[43].

- 3.9 The practical utility of purpose and principles provisions, however, largely depends on their form and design. Important considerations include the specificity of the goals, principles or policies set out in the provision, how they relate to one another, and their relationship to the more focused substantive provisions that follow.¹⁶ Significantly, there are no bright-line rules about how a purpose or principles provision should be framed.¹⁷

THE CASE FOR A PRINCIPLES PROVISION IN THE ACT

- 3.10 During the course of our review, it became apparent to us that many of the key aspects of search and surveillance law are contained in case law rather than the Act. The case law in this area has largely developed in relation to section 30 of the Evidence Act 2006 (which determines the basis on which improperly obtained evidence may be admissible in criminal proceedings)¹⁸ and section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA) (which protects against unreasonable search and seizure).
- 3.11 In discussing section 21 of NZBORA and section 30 of the Evidence Act, the courts have, on a number of occasions, identified relevant principles applicable to search and surveillance activity and have often placed constraints on how that activity is to be conducted.¹⁹ However, this is not evident on the face of the Search and Surveillance Act. That is problematic – it is arguably inconsistent with the law enforcement values of simplicity and certainty and with the rule of law, which requires the law to be accessible.
- 3.12 Given that the case law contains discernible and settled principles governing search and surveillance activity, we consider that it would be desirable for those principles to be imported into the Search and Surveillance Act. Such an approach would align with a comment that we received from judges of the senior courts that the Act would benefit from the identification of the legislation’s underlying principles and policies.²⁰ It would also address some general concerns raised in submissions about the level of training and experience of non-judicial issuing officers, and whether sufficient scrutiny is given to warrant applications.

16 In general, purpose and principles provision will not be useful if: they are expressed too narrowly (for example, by simply stating the *effect* of an Act); they are expressed too broadly (for example, by stating the social or economic goals of an Act, in a way that amounts to no more than a “political manifesto”); the interrelationship between purpose/principles provisions and the more focused substantive provisions in the Act is not made clear; or the principles of an Act conflict with each other and the Act does not specify which of those principles is to prevail. See *Burrows and Carter*, above n 2, at 238; JD Heydon “The ‘Objective’ Approach to Statutory Construction” (Supreme Court of Queensland Seminar, 8 May 2014) at 17; Oliver Jones (ed) *Bennion on Statutory Interpretation* (6th ed, LexisNexis, United Kingdom, 2013) at 684; Berry “Purpose Sections”, above n 11, at 57; and *Halsbury’s Laws of Canada* (online looseleaf ed, LexisNexis) at [HLG-16].

17 For example, while it may be undesirable, in general, to draft a principles provision with no internal hierarchy, there may be some situations (like in the Sentencing Act) where a broad, evaluative exercise is called for (see the Sentencing and Parole Reform Bill 2002 (148-2) (select committee report) at 6). In those circumstances, it may not be appropriate for the Act to imply that any one of the principles must be given greater weight than another.

18 We note that the case law in the search and surveillance context reflects only one aspect of s 30, and as we noted earlier in this Report, the Law Commission is currently considering the operation of s 30 in the context of its second statutory review of the Evidence Act.

19 For example, the courts have repeatedly emphasised that warrants and orders should be as specific as reasonably possible, and that searches need to be executed in a minimally intrusive manner: see the discussion in Chapter 4 at paragraphs [4.62]–[4.68].

20 The senior courts are the High Court, Court of Appeal and Supreme Court (see the Senior Courts Act 2016).

- 3.13 We envisage that a principles provision would set out the relevant considerations that need to be taken into account by persons exercising powers and functions under the Act.²¹ In our view, such a provision would:
- Provide better guidance for issuing officers and enforcement officers on how their powers and functions under the Act should be exercised as a matter of best practice.
 - Provide greater transparency to the general public on the considerations that are taken into account when search and surveillance activity is conducted.²²
 - Ensure the considerations and principles identified in the case law are addressed in advance of search and surveillance activity, rather than only being considered in hindsight during the “back-end” section 30 admissibility inquiry.²³ This would promote the proactive protection of individuals’ privacy rights and could contribute to a reduction in the number of subsequent challenges to the exercise of search and surveillance powers.
- 3.14 In many respects, we consider that the principles provision would act much like the principles in the Sentencing Act 2002.²⁴ It would perform an important accessibility and transparency function to both the users of the Act as well as the general public.
- 3.15 The inclusion of principles would also provide a flexible solution to two specific problems that we identified in our Issues Paper and discuss in more detail in Chapter 4:
- Our Issues Paper raised the question of whether the Act should be amended to introduce a general requirement to carry out search and surveillance activity pursuant to a warrant. We came to the view that it was desirable for positive authorisation to be sought before conducting search and surveillance activity; but did not consider it was possible to formulate a bright line statutory rule.²⁵
 - Our Issues Paper raised the question of whether the Act should be amended to expressly limit the use of warrantless powers to situations where it is not practicable to obtain a warrant. Ultimately we were concerned about the potential impact of such a prescriptive rule, as failure to comply with the rule would render the exercise of the power unlawful.²⁶ We did not think this was appropriate.

21 Although we did not have the benefit of receiving submissions on our proposed principles provision, we did discuss our proposals with our Officials Group and Expert Advisory Group. Some members of the Officials Group were concerned that a principles provision would amount to a set of mandatory rules (a concern that we address below at paragraphs [3.21]–[3.24]). Several members of the Expert Advisory Group expressed general support for a principles provision. They considered it would be of assistance to both enforcement and issuing officers.

22 This is an important function in the context of an Act that empowers State intrusions into the lives of individuals. The heated public discussion during the Search and Surveillance Bill’s passage demonstrated a high level of public concern about the State’s use of search and surveillance powers, and as we described in Chapter 2 at paragraph [2.37], the results of recent surveys on attitudes towards privacy in New Zealand suggest that public concern about privacy remains high.

23 As we discussed in Chapter 2, s 30 of the Evidence Act does not proactively protect individuals’ privacy rights because it only provides a means of determining—after the fact—the lawfulness and reasonableness of search and surveillance activity. It also only provides an avenue for challenging the legitimacy of that activity where charges are laid and the case proceeds to trial. In addition, because s 30 does not automatically result in the exclusion of improperly obtained evidence, it cannot be relied on as a way to hold enforcement officers to account for unlawful or unreasonable searches. Outside of s 30, individuals who have been the subject of search or surveillance activity can potentially challenge the legitimacy of that activity by: bringing an application for judicial review (see, for example, *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523); seeking a declaration and/or an award of damages for a breach of the New Zealand Bill of Rights Act 1990 (see, for example, *Henderson v Attorney-General* [2017] NZHC 606); applying for a stay of proceedings (see, for example, *R v T* [2016] NZDC 21847); and (in respect of police activity) making a complaint to the Independent Police Conduct Authority (see, for example, “Complaint of excessive use of force and unlawful entry to property in New Plymouth” (26 November 2015) available at < www.ipca.govt.nz >). Those forms of review suffer from the same limitation as s 30, in that they can only address the lawfulness and reasonableness of search and surveillance activity after the fact.

24 Sentencing Act 2002, s 8.

25 See paragraphs [4.16]–[4.27].

26 See paragraphs [4.37]–[4.43].

- 3.16 In our view, the discretionary nature of both the granting and manner of execution of a warrant or order underscores the suitability of including general principles in the Act, as opposed to specific statutory rules. The need for flexibility in this area has been repeatedly emphasised by the courts, particularly in relation to how the “reasonableness” assessment is to be conducted under section 21 of NZBORA.²⁷

THE PRINCIPLES PROVISION

The seven principles

- 3.17 We recommend that persons exercising functions and powers under the Act be required to take into account the following principles:
- *Principle 1:* conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement;²⁸
 - *Principle 2:* a warrant or order should be obtained in preference to exercising a warrantless power;
 - *Principle 3:* State intrusion into an individual’s privacy should be proportionate to the public interest in the investigation and prosecution of the offence or the maintenance of the law;
 - *Principle 4:* powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected;
 - *Principle 5:* powers under the Act should be exercised having regard to te ao Māori (the Māori dimension) and any other relevant cultural, spiritual or religious considerations;
 - *Principle 6:* powers under the Act should be exercised in a manner that minimises the impact on children and vulnerable members of the community; and
 - *Principle 7:* powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any individual.
- 3.18 We explain our reasons for settling on these seven principles in Chapter 4.

How the principles provision would operate

- 3.19 The principles provision we recommend is intended to set out relevant considerations that need to be taken into account by persons exercising powers and functions in the Act.
- 3.20 We wish to emphasise three points about the proposed operation of our principles provision. First, the principles we suggest are ones that we consider already underpin the Act and that have been stated in case law.²⁹ In short, it is not our intention to recommend a principles section

²⁷ The courts have made it clear that the reasonableness inquiry involves balancing individuals’ privacy interests against the public interest in law enforcement (see, for example, *R v Jefferies* [1994] 1 NZLR 290 (CA) at 319 per Thomas J). This approach has been described as principles-based: rather than creating fixed categories of unreasonable behaviour, or “bright line” tests of official misconduct, the courts have opted for “a flexible, case-by-case approach” that weighs all the relevant values and public interests involved: Scott Optican “Search and Seizure” in Grant Huscroft and Paul Rishworth (eds) *Rights and Freedoms* (Brookers Ltd, Wellington, 1995) 297 at 320 and 323. See also *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 (CA) at [209]–[222] and [224] per William Young P and Glazebrook J; *Television New Zealand Ltd v Attorney-General* [1995] 2 NZLR 641 (CA) at 647–648; and *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 (SC) at [194]. This flexibility is necessary because the focus under section 21 is on “the particular case in question not on the generality of police and other official searches. The decision turns on the unique circumstances of the particular case”: *R v Jefferies* [1994] 1 NZLR 290 (CA) at 304 per Richardson J. See also *Baron v Canada* [1993] 1 SCR 416 at 437.

²⁸ In Chapter 5, we explain what we mean by “policy statement”. In brief, we recommend that policy statements should be issued in relation to certain types of lawful activity, to provide guidance on when that activity is likely to be appropriate and how it should be carried out.

²⁹ With the exceptions of principles 5 and 6, which have not been the subject of direct consideration by the New Zealand courts. Instead, as we explain in Chapter 4, we consider that principle 5 is consistent with s 5(b) of the Act and several provisions in the New Zealand Bill of Rights Act 1990 (see paragraph [4.81]) and principle 6 can be inferred from the case law on minimising privacy intrusions (see n 116 in Chapter 4).

- that creates any new legal obligations. It is evident from the case law that these considerations should already be taken into account when search and surveillance powers are exercised and that a failure to do so may result in search or surveillance activity being held to be unreasonable in terms of section 21 of NZBORA.
- 3.21 Second, the decision as to whether a warrant or order is issued and whether and how powers under the Act are exercised should remain a discretionary, evaluative exercise.³⁰ As such, the principles are not intended to prescribe substantive outcomes that must be guaranteed in any given case. They are not mandatory rules.
- 3.22 By way of example, the courts have emphasised that search and surveillance powers should be executed in a minimally intrusive manner (and we have drawn on that case law in developing our recommendation to include principle 4).³¹ However, if a search is in fact executed in an overly broad manner, a court will not necessarily find that it was unreasonable in terms of section 21. The reasonableness assessment is a context-specific inquiry that requires consideration of the particular facts and circumstances in each individual case.
- 3.23 We therefore envisage that non-compliance with a principle will be a relevant (but not determinative) factor that is considered by the courts when assessing reasonableness under section 21 of NZBORA.³² We expect (as is already the case) that a significant departure from the principles may mean that a court will find the search or surveillance activity to be unreasonable.³³ Equally, the fact that a warrant and its execution complied with the principles would be relevant when it comes to evaluating the reasonableness of the activity.³⁴
- 3.24 We considered whether the principles provision should explicitly state that conduct carried out in a manner inconsistent with the principles is not automatically rendered invalid, unlawful or unreasonable.³⁵ However, on reflection, we did not consider this to be necessary because we have framed our proposed principles as relevant *considerations* that must be taken into account. The fact that conduct is not automatically rendered invalid, unlawful or unreasonable if it is carried out in a manner inconsistent with the principles therefore will already be apparent from the provision.

30 *Gill v Attorney-General* [2011] 1 NZLR 433 (CA) at [36]; *New Zealand Air Line Pilots' Association Inc v Attorney-General* [1997] 3 NZLR 269 (CA) at 292.

31 See, for example, *R v Ririnui* [1994] 2 NZLR 439 (CA) at 442; *R v Briggs* [1995] 1 NZLR 196 (CA) at 202; and *R v Hapakuku* (1999) 16 CRNZ 520 (CA) at 525.

32 We also note that, in theory, an application could be brought by way of judicial review on the basis of an 'error of law' (for example, by applicants arguing that an issuing officer failed to take into account a mandatory consideration listed in the principles provision) or *Wednesbury* unreasonableness (see *Associated Provincial Picture Houses Ltd v Wednesbury Corporation* [1948] 1 KB 223, [1947] 2 All ER 680). We do not consider the inclusion of a principles provision will have the unintended effect of increasing such litigation before an investigation has finished or before charges are laid. This is because there are significant constraints on the ability to bring an application for judicial review in that context. The courts will only entertain challenges by way of judicial review where there is a defect in the search warrant 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: *Gill v Attorney-General* [2010] NZCA 468; [2011] 1 NZLR 433 at [20], confirmed in *Southern Storm Fishing (2007) Ltd v Chief Executive, Ministry of Fisheries* [2015] NZCA 38, [2015] NZAR 816 and *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523 at [58].

33 See similar observations in relation to the guidance as to best practice for those who apply for search warrants provided in *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 (CA) at [225] per William Young P and Glazebrook J.

34 See similar observations in *Television New Zealand Ltd v Police* [1995] 2 NZLR 541 (HC) at 550.

35 There are some examples of statutes in New Zealand that include principles provisions, and then go on to expressly explain the legal effect of those principles. For example, s 11 of the Policing Act 2008 specifically provides that the principles in the Act do not in themselves impose "particular duties" on New Zealand Police; s 31(4) of the Sentencing Act 2002 provides that the fact a court has omitted to refer to a particular sentencing principle is not itself grounds for appeal; and s 11 of the Privacy Act 1993 expressly states that the information privacy principles in s 6 of the Act do not give rise to legally enforceable rights outside the Act, with the one exception of principle 6(1) (see also *R v A* [2017] NZSC 42 at [37]). Most statutes with principles provisions are silent as to the legal effect of failing to comply with a principle. In those situations, whether non-compliance is fatal to the validity of an exercise of functions or powers under an Act will depend on the view the courts take of non-compliance in the statutory context. The applicable principles of administrative law were set out in *Wang v Minister of Internal Affairs* [1998] 1 NZLR 309 (HC) at 318.

3.25 Finally, we have suggested framing the principles as considerations that must be taken into account when exercising powers and functions under the Act³⁶ rather than describing them as principles that underpin the Act (which is a formulation seen in some other legislation, for example, section 8 of the Policing Act 2008).³⁷ This is because the principles are intended to specifically guide the exercise of decision-making under the Act rather than simply articulating the underlying values of the legislation or acting as an interpretive aid.³⁸

Should the principles apply to all search and surveillance powers?

3.26 We consider that the first principle (that conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement) should apply to all enforcement officers.³⁹ This is because the aim of the principle is to encourage enforcement officers to make use of available warrants and statutory powers, both under the Act and when operating under their own legislation.

3.27 However, we consider that the remaining principles should apply to enforcement officers and issuing officers only when exercising powers under the Search and Surveillance Act itself (not legislation listed in the Act's Schedule). This is because the principles do not sit comfortably with many of the regulatory powers available to enforcement agencies. For example, a proportionality assessment may not be workable in the context of an inspection power that does not depend on the existence of a threshold before it is exercised.⁴⁰

3.28 There is another matter that we need to clarify. We note that some of the principles we recommend have been framed as applying when “powers under the Act are exercised” (principles 4–7). In Chapter 5, we recommend that policy statements should be issued in relation to certain types of activity to provide guidance on when that activity is likely to be appropriate and how it should be carried out. Policy statements would need to reflect, and be consistent with, the principles we recommend in Chapter 4. However, we acknowledge that an enforcement officer acting in accordance with a policy statement is not, strictly speaking, exercising “a power under the Act”. Accordingly, the principles are relevant to an activity covered by a policy statement but in a more indirect way.

The process of applying for a warrant or order

3.29 We envisage that—to give effect to a number of the principles we propose—enforcement officers will likely include information relating to the principles in their applications for warrants or orders under the Act. For example, to give effect to the principle that powers under the Act should be exercised in a manner that protects privilege (principle 7), we expect that applications for warrants and orders will signal when issues of privilege may arise and contain sufficient information to enable issuing officers to make informed decisions (for example, about whether to issue the warrant or order at all, or whether conditions need to be imposed).

36 We refer by way of example to s 4 of the Care of Children Act 2004, which states: “(2) Any person considering the welfare and best interests of a child in his or her particular circumstances—(a) must take into account—(i) the principle that decisions affecting the child should be made and implemented within a time frame that is appropriate to the child's sense of time; ...”.

37 Section 8 of the Policing Act 2008 sets out a number of principles that the Act “is based on”. As noted above at n 35, the principles do not impose any particular duties on Police or any police employees (s 11).

38 See the description of the various functions that can be performed by a principles provision at paragraph [3.7].

39 We use the term “enforcement officers” as it is defined in s 3 of the Act: “a constable; or ... any person authorised by an enactment specified in column 2 of the 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”.

40 That said, as we explained in Chapter 2 at paragraph [2.84], we see value in the Ministry of Justice conducting a separate stream of work that considers the extent to which the Act can appropriately be applied to regulatory agencies, including the extent to which the principles we identify in Chapter 4 are applicable to the powers listed in the Act's Schedule.

3.30 We considered whether the Act should require applicants to include this information. We decided against such an approach because we did not consider the types of information that may be relevant to the principles were capable of rigid classification. Instead, we recommend that issuing officers should have the ability to request further information from an applicant in order to determine whether and how any principle might apply. We note that the Act already permits an issuing officer to require an applicant to supply further information concerning the grounds on which a search warrant is sought.⁴¹

Training

3.31 As we have stated, our recommendation to include a principles provision does not envisage the creation of new obligations. For that reason, we do not anticipate that the provision will be particularly burdensome for enforcement agencies and issuing officers to apply. We acknowledge, however, that our recommendation for the Act to include a principles provision will require enforcement officers and issuing officers to undertake training on the principles and the practical steps required to take them into account when making applications for warrants and orders under the Act, assessing those applications, and exercising powers under the Act.

RECOMMENDATIONS

- R3 A principles section should be inserted into the Act.
- R4 Section 98(2) (relating to requirements for further information) should be amended to permit an issuing officer to require an applicant for a warrant or order to supply further information concerning whether and how any of the principles apply.

41 Search and Surveillance Act 2012, s 98(2)(a).

Chapter 4

The principles

INTRODUCTION

- 4.1 In this chapter, we set out our reasons for recommending the inclusion of the following principles in a provision in the Search and Surveillance Act 2012 (the Act):
- *Principle 1:* conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement;
 - *Principle 2:* a warrant or order should be obtained in preference to exercising a warrantless power;
 - *Principle 3:* State intrusion into an individual's privacy should be proportionate to the public interest in the investigation and prosecution of the offence or the maintenance of the law;
 - *Principle 4:* powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected;
 - *Principle 5:* powers under the Act should be exercised having regard to te ao Māori (the Māori dimension) and any other relevant cultural, spiritual or religious considerations;
 - *Principle 6:* powers under the Act should be exercised in a manner that minimises the impact on children and vulnerable members of the community; and
 - *Principle 7:* powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any individual.
- 4.2 In the course of doing so, we address several issues that we raised in our Issues Paper, for example: whether the Act should be more specific about when a warrant is required; whether the Act should expressly limit the use of warrantless powers in the Act to situations where it is not practicable to obtain a warrant; and whether the Act adequately protects privileged material during the exercise of search or surveillance powers.

PRELIMINARY ISSUES

Drafting issues

- 4.3 The precise language used in a principles provision is of crucial importance. The one-year timeframe for our review meant it was not possible to ask the Parliamentary Counsel Office for assistance with even an indicative clause. We therefore anticipate that the exact wording of the principles will require refinement during the drafting process. Our discussion of the content of the seven principles we recommend in this chapter is intended to provide a starting point.

The value of law enforcement

- 4.4 The principles we recommend are primarily aimed at promoting and protecting human rights values. During the course of our review, we considered whether there should be a stand-alone principle that explicitly recognises the value of law enforcement.¹ Given that the purpose of the Act (in section 5) recognises two sets of values in the context of regulating search and surveillance powers (human rights values and law enforcement values), we could see the attraction of including such a principle.
- 4.5 On reflection, we concluded this was unnecessary. While section 5 of the Act recognises the need to ensure “investigative tools are effective and adequate for law enforcement”, in our view, that purpose is already reflected in the numerous provisions in the Act that empower enforcement agencies to conduct search and surveillance activity. Those provisions constitute Parliament’s recognition that certain State intrusions into privacy are justified in light of law enforcement imperatives. Furthermore, law enforcement is already recognised in statute as a core function of Police in section 9 of the Policing Act 2008.² Section 8 of that Act also sets out a number of principles that the Act is based on, including the principle that “principled, effective, and efficient policing services are a cornerstone of a free and democratic society under the rule of law”.³ In our view, further explication of the value of law enforcement in the Search and Surveillance Act is not needed.

PRINCIPLE 1: USING STATUTORY MECHANISMS TO CARRY OUT INTRUSIVE ACTIVITY

- 4.6 The first principle that we recommend for inclusion is “the principle that conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement”.

Background

- 4.7 The basis for this recommendation stems from Chapter 2 of our Issues Paper, where we asked submitters whether the Act should be more specific about when a warrant is required.⁴ We explained in our Issues Paper that 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.⁵ Rather, it is left to enforcement officers to determine on a case-by-case basis whether the proposed activity is likely to amount to a “search” in terms of section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA).

1 We note that the proportionality principle we recommend (principle 3) acknowledges both the public interest in protecting individuals’ privacy as well as the legitimate interest that law enforcement agencies have in the investigation and detection of crime.

2 Policing Act 2008, s 9(c). We also note that law enforcement is not necessarily a principal function of non-Police enforcement agencies that exercise powers under the Search and Surveillance Act: for example, see the regulatory objectives set out in s 16 of the Food Act 2014, which is administered by the Ministry for Primary Industries.

3 Section 8(a).

4 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) question 1 [Issues Paper].

5 Section 6.

- 4.8 Whether conduct amounts to a “search” in terms of section 21 depends on whether the activity amounts to a State intrusion on reasonable expectations of privacy.⁶ We noted that the concept of “reasonable expectations of privacy” can be difficult to apply and that this generates uncertainty for enforcement officers as to when they need to obtain a warrant.⁷ A separate concern is that—without requiring positive authorisation to conduct a search—the Act does not provide a high degree of assurance to the public that their privacy interests are being adequately and proactively protected.⁸
- 4.9 As for the Act’s surveillance device warrant regime, the Act requires enforcement officers to obtain a surveillance device warrant before conducting certain types of surveillance.⁹ However, in relation to surveillance that is not covered by that regime, the Act does not specifically require enforcement officers to obtain prior authorisation. Nor does it provide the means for enforcement officers to obtain a warrant in such cases. In practice, if enforcement officers wish to undertake surveillance activity not covered by the Act, they need to determine on a case-by-case basis whether the proposed activity is likely to amount to a “search” in terms of section 21 of NZBORA.¹⁰
- 4.10 We noted that when the Law Commission wrote its 2007 Report, *Search and Surveillance Powers*, it had intended any law enforcement activity that might invade a reasonable expectation of privacy to be carried out pursuant to a warrant. To reflect that policy, it recommended the introduction of a “residual warrant” regime, which would have required authorisation by warrant for intrusive actions not covered by other provisions.¹¹ The introduction version of the Bill largely adopted that recommendation.¹² However, concerns were expressed during the Select Committee stage about the residual warrant regime (which we describe in more detail in Chapter 6). This resulted in the regime being removed and replaced with a declaratory order regime.¹³
- 4.11 The declaratory order regime provides a mechanism for enforcement officers to receive—in advance of using investigatory methods not expressly covered by the Act—some level of assurance that the use of devices or techniques are lawful and reasonable. An enforcement officer can apply for a declaratory order if they wish 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”.¹⁴ If a judge is satisfied the proposed course of action

6 See *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [163] per Blanchard J, together with *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22]; and more recently, *R v A* [2017] NZSC 42 at [50]. The word “search” also carries its ordinary meaning in the sense of “consciously looking for something or somebody”: see *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [220] per Tipping J. See also at [164], where Blanchard J referred to the idea of an “investigation or scrutiny in order to expose or uncover”; and *W v R* [2016] NZCA 580 at [20]–[33]. The Court of Appeal recently observed that, in many cases, the fact of a search will be reasonably obvious (that is, involving physical acts of prying into hidden places); although there will be cases where a non-physical intrusion qualifies (for example, surveillance of private spaces): *Wright v Bhosale* [2016] NZCA 593 at [45]. We note that in *Wright*, the Court of Appeal considered the issue of whether police questioning could ever amount to a “search”. The Court rejected the general proposition that questioning by a police officer constitutes an intrusion into privacy, but acknowledged that (in certain circumstances) such questioning could amount to a search (for example, if private information is unwillingly disclosed to the State): see at [46] and [49]–[50]. The Court emphasised that whether the conduct of Police constitutes a search was a “fact-specific inquiry” (at [45]).

7 Issues Paper, above n 4, at [2.78].

8 At [2.82].

9 Search and Surveillance Act 2012, s 46.

10 Although the Search and Surveillance Act 2012 differentiates between searches and surveillance activity for authorisation purposes, they are treated the same in terms of s 21. So the reasonable expectations of privacy test for determining whether activity amounts to a search may equally capture conduct that might be classed as surveillance.

11 See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) recommendation 11.24. The Commission considered that such a regime would “reinforce the presumptive requirement that all search, seizure, interception and surveillance activity be conducted pursuant to warrant” (at [11.131]).

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

13 Search and Surveillance Bill 2009 (45-2), cls 57–61.

14 Search and Surveillance Act 2012, s 66.

is lawful and reasonable, the order may be issued.¹⁵ The order is advisory in character and does not bind subsequent courts.¹⁶ In our Issues Paper, we noted that one of the drawbacks of the regime was that the orders are indicative only so may not provide enforcement officers with a particularly high level of assurance that they are acting lawfully and reasonably.¹⁷

- 4.12 Our Issues Paper set out a number of alternatives to the Act’s current approach, which could help clarify when a warrant should or must be obtained: introducing an optional residual warrant regime; introducing a mandatory residual warrant regime; or requiring authorisation for all search and surveillance activities.¹⁸ We noted that—if the second or third options were adopted—the Act would also need to define what type of conduct requires authorisation.¹⁹
- 4.13 Some of the issues that we raised are dealt with in subsequent chapters of this Report.²⁰ The focus of our discussion in this chapter is on the overarching issue of whether it is appropriate to introduce a statutory rule requiring positive authorisation for all search and surveillance activity.

Submissions

- 4.14 The submissions we received were split on whether the Act should be more specific about when a warrant is required. In general, enforcement agencies tended to oppose the idea, while other submitters (including the Human Rights Commission, New Zealand Law Society and New Zealand Criminal Bar Association) supported it.
- 4.15 Amongst those submissions in favour of clarifying when authorisation is required, there was no clear consensus on how this could work in practice. Most submitters favoured using “reasonable expectations of privacy” as the statutory test. Te Hunga Rōia Māori o Aotearoa and the Human Rights Commission suggested a similar but slightly lower threshold of requiring authorisation whenever privacy rights or interests *might* be engaged.

Our recommendation

- 4.16 In our view, the primary advantage of a statutory rule requiring positive authorisation for search and surveillance activity is that it would guarantee consideration is given to individuals’ privacy interests before intrusive activity is carried out.
- 4.17 However, we became concerned that an appropriate bright line—delineating the types of activity that do and do not require legal authorisation—could not be drawn. We reached the view that any test that would be broad enough to be of general application, such as the “reasonable expectations of privacy” test, was likely to lack sufficient certainty to form the basis of a statutory requirement.
- 4.18 The right in section 21 of NZBORA to be free from unreasonable search or seizure recognises a spectrum of circumstances in which individuals may have a reasonable expectation of privacy. It is “impossible to lay down a comprehensive list of discrete circumstances and hold that a reasonable expectation of privacy exists (or not) in respect of each”.²¹ Rather, an assessment has

15 Section 65(1).

16 Section 65(2).

17 Issues Paper, above n 4, at [2.79].

18 At [2.89].

19 This could be based on the “reasonable expectations of privacy” test, or an alternative threshold could be adopted. We set out an alternative test in our Issues Paper, above n 4, at [2.117].

20 For example, in Chapter 6, we explain why we have not recommended replacing the declaratory orders regime with a residual warrant regime (and address concerns expressed by the judiciary that declaratory orders are akin to advisory opinions: see paragraphs [6.26] and [6.50]–[6.57]) and in Chapter 7, we recommend amending the surveillance device warrant regime to cover a wider range of activity.

21 Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis, Wellington, 2015) at [18.10.2].

to be made by reference to a range of factors.²² For that reason, we considered that introducing a requirement to obtain legal authorisation for search and surveillance activity would create more problems than it would solve, as it would still require enforcement officers to apply a vague standard in determining whether to obtain a warrant.

4.19 We were also concerned about the incidental effect of a statutory rule requiring positive authorisation on the constitutional notion that the Government has the freedom to do anything that is not prohibited by law. The existence of this “third source”²³ of authority has been recognised in some judicial decisions,²⁴ and has also received some support in academic writing.²⁵ In short, the third source provides State actors with all the powers that a natural person has, provided that the use of those powers does not conflict with legislation, the common law, or breach protected rights.²⁶ In addition, the third source cannot provide authority for executive action where the field of that action is circumscribed by statute (where legislation “covers the field”).²⁷

4.20 In *Ngan v R*, McGrath J observed that there were “strong practical reasons for accepting the existence of [this] residual freedom”:²⁸

[T]housands of government actions take place every day under this form of legal authority. Most are administrative and free from controversy, as they have no impact on the legal rights of citizens. Unless a residual freedom to act is recognised, there will be doubt over legal validity. Requiring prior parliamentary authority generally or in relation to certain types of actions can in theory provide desirable democratic legitimacy, and also better legal certainty, but there are logistic difficulties in making that approach work. Codification of all government power would be a huge task and, if attempted, many powers would inevitably be so broadly expressed as to make the democratic advantages illusory.

4.21 If the Act were to require a warrant to be obtained before carrying out activity that amounts to a State intrusion on reasonable expectations of privacy (in other words, a “search” in terms of section 21 of NZBORA), the consequence of failing to do so is that the activity would automatically be unlawful. This would appear to represent a departure from current New Zealand case law, where at least some judges have expressed the view that a search may

22 The variability of “reasonable expectations of privacy” has been commented on in a number of Court of Appeal decisions. For example, in *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA) at 407, the Court observed that “[a]n assessment of the seriousness of the particular intrusion involves considerations of fact and degree, not taking absolutist stances”. See also *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 (CA) at [113] and *R v Jefferies* [1994] 1 NZLR 290 (CA) at 302.

23 The other two sources of authority—statute and the prerogative—are uncontroversial and widely recognised.

24 *Minister for Canterbury Earthquake Recovery v Fowler Developments Ltd* [2013] NZCA 588, [2014] 2 NZLR 587 at [82]–[83], referring to the judgments of McGrath J in *Ngan v R* [2007] NZSC 105, [2008] 2 NZLR 48 at [93]–[100] and *Rogers v Television New Zealand Ltd* [2007] NZSC 91, [2008] 2 NZLR 277 at [110], and Tipping J in *Ngan* at [45] and *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [217]. Compare the contrary view of Elias CJ in *Hamed* at [24]. This point was left open on appeal in *Quake Outcasts v Minister for Canterbury Earthquake Recovery on appeal from Minister for Canterbury Earthquake Recovery v Fowler Developments Ltd* [2015] NZSC 27, [2016] 1 NZLR 1 at fn 152.

25 See B V Harris “Recent Judicial Recognition of the Third Source of Authority for Government Action” (2014) 26 NZULR 60. For the contrary view, see Philip Joseph *Constitutional and Administrative Law in New Zealand* (4th ed, Brookers Ltd, Wellington, 2014) at [18.3.3]; Graham Taylor *Judicial Review: A New Zealand Perspective* (3rd ed, online ed, LexisNexis, Wellington, 2014) at [2.30]–[2.32]; and Butler and Butler, above n 21, at [18.5.6] and [18.20.5].

26 *Ngan v R* [2007] NZSC 105, [2008] 2 NZLR 48 at [97] per McGrath J: “In particular the residual freedom of officials is constrained by the Bill of Rights Act. Residual freedom to act can never justify a breach of protected rights”.

27 See *Minister for Canterbury Earthquake Recovery v Fowler Developments Ltd* [2013] NZCA 588, [2014] 2 NZLR 587 at [79], referring to *Attorney-General v De Keyser’s Royal Hotel Ltd* [1920] AC 508 (HL) at 539–540 per Lord Atkinson. On appeal, the Supreme Court agreed with the Court of Appeal’s conclusion that the Act covered the field: *Quake Outcasts v Minister for Canterbury Earthquake Recovery on appeal from Minister for Canterbury Earthquake Recovery v Fowler Developments Ltd* [2015] NZSC 27, [2016] 1 NZLR 1 at [112].

28 *Ngan v R* [2007] NZSC 105, [2008] 2 NZLR 48 at [96].

still be lawful and reasonable in terms of section 21 even if there was no express authority to conduct it.²⁹

- 4.22 We would not want to suggest a shift from this approach to one where enforcement officers require specific authority to carry out certain types of activity if we cannot draw a bright line between what does and does not require authorisation. In our view, such a shift could have the unintended effect of calling into question a number of routine and uncontroversial activities that are carried out by State actors without positive authorisation. Furthermore, we are not convinced that such a shift in approach is one that should be made in the context of a review of the Search and Surveillance Act without broader consideration of whether this is required by the terms of NZBORA.³⁰
- 4.23 While we do not recommend a statutory rule requiring legal authorisation for search or surveillance activity, we do recommend the inclusion of a general principle that conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement.³¹
- 4.24 We consider that inclusion of this general principle will help to reinforce the importance of obtaining positive lawful authority for invasive actions where possible (or acting in accordance with a specific and transparent policy statement) while avoiding the drawbacks of having a mandatory statutory requirement. There is value in including such a principle given that the courts have, on a number of occasions, emphasised the importance of obtaining authorisation prior to conducting search and surveillance activity.³² For example, in *R v Williams*, Hammond J described the concept of judicial pre-authorisation as a preventative or “prophylactic” device against unjustified State intrusion.³³ He noted that meaningful judicial pre-authorisation

29 See *R v Gardiner* (1997) 15 CRNZ 131 (CA) at 134; *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [217] per Tipping J; and *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [26]–[38]. As the Court of Appeal observed in *Lorigan v R* at [38] (emphasis added), “the Search and Surveillance Act 2012 ... proceeds on an assumption that surveillance of a public place in a manner not involving trespass is lawful, and does not require a surveillance device warrant. Parliament appears to have legislated on the basis that *no statutory authorisation for such activity is necessary even if the surveillance is a search*”. We note that—in contrast—the approach adopted under the European Convention on Human Rights (the Convention for the Protection of Human Rights and Fundamental Freedoms 213 UNTS 222 (opened for signature 4 November 1950, entered into force 3 September 1953)) and Canadian Charter of Rights and Freedoms 1982 requires lawful authority for search and surveillance activity. The Convention recognises a right to privacy that can only be subject to restrictions that are “in accordance with law” (art 8). Section 8 of the Canadian Charter is similar in wording to s 21 of the New Zealand Bill of Rights Act 1990; however, the courts have held that searches not prescribed by law are presumptively unreasonable: see, for example, *R v Herbert* [1990] 2 SCR 151.

30 We note that those who argue that public officials do not have the freedom to act in any way they choose unless prohibited by law have sometimes relied on s 5 of the New Zealand Bill of Rights Act 1990, which states that the rights and freedoms in that Act may be subject only to reasonable limits that are “prescribed by law”. It has been suggested that this means that s 21 requires positive authority for intrusions upon personal freedom: see *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [35] per Elias CJ; and Butler and Butler, above n 21, at [6.12.18]–[6.12.20] and [18.20.4]–[18.20.9]. It has also been suggested that such an interpretation is necessary to give effect to art 17 of the International Covenant on Civil and Political Rights, which recognises the right to privacy. See *Hamed v R* at [36] and [41] per Elias CJ; and the arguments recorded in *R v Gardiner* (1997) 15 CRNZ 131 (CA) at 133–134. New Zealand’s commitment to the International Covenant is affirmed in the long title to the New Zealand Bill of Rights Act. There is force in these arguments; however, we consider there are two immediate complications. First, as we explained in Chapter 2, privacy is not explicitly recognised in the New Zealand Bill of Rights Act as a stand-alone right, and in the course of this review we have not considered whether it ought to be. Second, the courts’ approach to s 21 has been to consider the reasonableness of a search under s 21 itself rather than s 5: see *Cropp v Judicial Committee* [2008] NZSC 46, [2008] 3 NZLR 774 at [33] and *Hamed v R* at [162] per Blanchard J. That is not to say that the legitimacy of this position cannot be re-examined. However, we consider those issues are best considered in the context of any future review of the New Zealand Bill of Rights Act rather than in our limited review of the Search and Surveillance Act’s provisions.

31 “Order” in this context would include a production order, examination order, and declaratory order (or “order authorising specific activity”, as we suggest in Chapter 6) as well as similar production or examination orders available to regulatory agencies under their own empowering legislation. “Warrants” and “statutory powers” would include those available under the Act as well as warrants and powers of search, seizure, production and examination available to regulatory agencies under their own empowering legislation.

32 As a majority of the Supreme Court explained in *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 (SC) at [71]: “in general searches must be carried out under warrant, thus interposing the decision of an independent judicial officer between the investigators seeking to conduct a search and the suspect. Besides providing authority for a search and delineating its scope, a search warrant serves the important function of informing both the searchers and the searched of the legitimate scope of the search”. See also *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705 at [32]–[33].

33 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [263] per Hammond J. See also Butler and Butler, above n 21, at [18.16.6].

requires a neutral third party, capable of acting as a true intermediary between the rights of the individual and the interests of the State.³⁴

- 4.25 We emphasise that the aim of the principle is to encourage enforcement officers to make use of available statutory mechanisms, both under the Act itself and when operating under their own legislation. We acknowledge the principle employs the language of “reasonable expectations of privacy” and therefore presents a level of uncertainty regarding its application. However, later in this Report we make two recommendations that we consider will assist with the principle’s application.
- 4.26 First, in Chapter 5, we recommend that “policy statements” should be issued in relation to certain types of lawful activity³⁵ that may constitute an intrusion into reasonable expectations of privacy and therefore run the risk of being carried out unreasonably if not carried out in an appropriate manner.³⁶ The aim is for the statements to provide guidance on grey areas where it may be unclear whether a particular type of activity is lawful or appropriate in the absence of a warrant. As such, the statements are intended to address some of the difficulty in drawing a bright line between conduct that intrudes on a reasonable expectation of privacy and conduct that does not.
- 4.27 Second, in Chapter 6, we explain why we think that the declaratory order regime should be retained and propose some amendments to clarify the purpose and effect of such orders. These orders will allow enforcement officers to seek authorisation for activity where no specific warrant, order or power appears to be available (and the proposed activity may not be covered by a policy statement). In short, they provide a mechanism for enforcement officers to seek guidance on whether proposed activity that may constitute an intrusion into reasonable expectations of privacy is lawful and reasonable. In our view, the principle we have proposed would be unable to operate effectively unless such a mechanism exists. We expect that the amendments we propose to that regime, coupled with the introduction of this general principle, will encourage their greater use.

PRINCIPLE 2: WARRANT PREFERENCE

- 4.28 The second principle that we recommend is “the principle that a warrant or order should be obtained in preference to exercising a warrantless power”.

Background

- 4.29 The basis for this recommendation stems from Chapter 7 of our Issues Paper, where we asked submitters whether the Act should expressly limit the use of warrantless powers in the Act to situations where it is not practicable to obtain a warrant.³⁷
- 4.30 As we explained in the Issues Paper, there are a number of warrantless powers available to Police under the Act.³⁸ The underlying rationale for these warrantless powers is to allow Police

34 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [263] per Hammond J.

35 Either because the activity is permitted under the general law, or because they have been authorised under the Act.

36 In this Report we recommend that policy statements be issued for interception and tracking with consent (Chapter 9), specific types of public surveillance (Chapter 11), production orders (Chapter 14), and covert operations and the use of assumed identities (Chapter 15). These policy statements would provide guidance on how that activity should be carried out, and may also indicate situations in which it is preferable for a warrant or order to be obtained. Failure to act in accordance with a policy statement would not render an act unlawful or unreasonable: instead this could influence a court’s assessment of whether the activity was reasonable in terms of s 21 of the New Zealand Bill of Rights Act 1990.

37 Issues Paper, above n 4, at [7.15]–[7.28].

38 For example, warrantless powers of entry and search to preserve evidence (ss 8, 15–17, 25, 83, 84 and 88); of entry and search to make an arrest (ss 7–9); of entry to protect life and property (ss 11, 14, 85 and 88); to search for evidence of specific offences (ss 18–22 and 27–29) and to search places incidental to arrest or detention (s 11).

to respond to urgent circumstances. They are therefore available only in special cases where there is an overriding public interest in the granting of such a power.³⁹

- 4.31 Courts have repeatedly recognised the exceptional nature of warrantless powers, holding that the reasonable exercise of a lawful power to search without a warrant requires that the power is resorted to “only where it is reasonably necessary to do so before a warrant can be obtained”.⁴⁰ In other words, the lawful exercise of a warrantless power can be unreasonable in terms of section 21 of NZBORA if a warrant could have been readily obtained.⁴¹ For example, in *R v Laugalis*, the Court of Appeal held that a search conducted pursuant to a warrantless statutory power was unreasonable because there were no urgent circumstances and a warrant could have been applied for.⁴²
- 4.32 *Laugalis* has sometimes been described as endorsing a “warrant preference approach”: it is best practice for powers of search and entry to be exercised pursuant to a warrant, even where a warrantless power is available.⁴³ However, the courts have acknowledged that a “realistic and practical approach”⁴⁴ is required when assessing whether the situation faced by a police officer made it reasonable to invoke a warrantless power.⁴⁵
- 4.33 We noted in our Issues Paper that section 20 of the Search and Surveillance Act appears to be the only warrantless search power in the Act that explicitly adopts the warrant preference approach.⁴⁶ That section permits warrantless searches of places and vehicles in relation to certain Misuse of Drugs Act 1975 offences. It expressly 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. We asked for submitters’ views on whether all warrantless search powers under the Act should be limited in this way.⁴⁷

Submissions

- 4.34 Submitters were fairly evenly split on whether the Act should expressly limit the use of warrantless powers to situations where it is not practicable to obtain a warrant. The submitters who supported this (including the New Zealand Law Society, Auckland District Law Society Inc and New Zealand Criminal Bar Association) were of the view that it would reinforce the importance of using warrantless powers in exceptional circumstances only.
- 4.35 One submitter suggested that it would ensure that proper regard is had to the existence of section 117 of the Act, which provides enforcement officers with a power to secure evidence at an intended search scene while an application for a search warrant is being processed. That

39 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at 22. The Commission described warrantless powers as an “exception to the general rule that searches by law enforcement officers may only be undertaken pursuant to the terms of a warrant issued by an independent officer acting judicially”: at [5.1].

40 *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA) at 408.

41 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [24]; *R v Laugalis* (1993) 10 CRNZ 350 (CA) at 355–356; *R v H* [1994] 2 NZLR 143 (CA) at 148.

42 *R v Laugalis* (1993) 10 CRNZ 350 (CA) at 355–356.

43 *SF v R* [2014] NZCA 313 at [46]; *K v R* [2016] NZCA 259 at [44]; *R v McGarrett* [2016] DCR 175 at [89]; *Police v Davies* [2016] DCR 165 at [33] and [35].

44 *F v R* [2014] NZCA 313 at [46].

45 As the Court of Appeal observed in *R v Williams*, “[r]egard must be had to the practicalities of policing, including whether a property can be kept under surveillance, and the resources available to officers at that time”: *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [24].

46 Issues Paper, above n 4, at [7.22]. While strictly speaking not a “search” power, we note that a similar approach is adopted in s 48 of the Search and Surveillance Act 2012, which provides for warrantless surveillance to be conducted in certain situations of emergency or urgency. Section 48(1)(b) states that the warrantless surveillance cannot be carried out unless “obtaining a surveillance device warrant within the time in which it is proposed to undertake the surveillance is impracticable in the circumstances”.

47 Issues Paper, above n 4, at [7.25].

submitter suggested the availability of section 117 reduces the need for the immediate exercise of warrantless search powers in some circumstances.⁴⁸

- 4.36 The submitters who were opposed to the idea said it was unnecessary, because the warrant preference approach is already sufficiently recognised through the existing preconditions for exercising warrantless powers. An element of urgency is assumed in those preconditions. It was also suggested that such a requirement would substantially increase the burden on courts and on Police to prepare warrants where there would be little or no benefit in obtaining a court's oversight. One submitter did not agree that the courts have accepted that a warrant preference approach applies beyond section 20 of the Act so as to apply to the exercise of any warrantless power under the Act.

Our recommendation

- 4.37 We acknowledge that the existing preconditions for exercising warrantless powers under the Act already assume an element of urgency. However, we do not think those preconditions go far enough to reflect the warrant preference approach. While the warrantless powers in the Act reflect Parliament's acceptance that, in general, there are some urgent circumstances that justify the use of search powers without a warrant, that does not mean the exercise of such powers will be necessary and reasonable in every case where the statutory preconditions are met. There may be cases (albeit rare) where it is nonetheless practicable to obtain a warrant.
- 4.38 By way of example, section 18(3) of the Act permits a constable to enter a house without a warrant and search for firearms where there are reasonable grounds to suspect there are firearms inside that may be evidential material in relation to an offence against the Arms Act 1983. The rationale for this warrantless power is that firearms pose an immediate threat to public safety and the safety of individuals in the immediate vicinity.⁴⁹ However, it is possible to think of situations where the requirements of section 18(3) are satisfied, but it is nevertheless practicable to obtain a warrant before the power of entry and search is exercised. For example, if the constable knows that the occupants of the house are overseas, we consider it is at least arguable that a search under section 18(3) could be found to be unreasonable.⁵⁰
- 4.39 We see no reason why the warrant preference approach should apply only to the exercise of section 20 of the Act. It is a well-established principle that not all lawful searches are reasonable and that an otherwise lawful search may still be unreasonable in terms of section 21 of NZBORA where a warrant was readily obtainable and there was no true urgency.⁵¹ While many of the cases in this area have been concerned with warrantless searches of places and vehicles in relation to Misuse of Drugs Act offences, we are of the view that this general principle has broader application to all warrantless powers under the Act.
- 4.40 For those reasons, we recommend the inclusion of a general principle in the Act that a warrant should be obtained in preference to exercising a warrantless power. In our view, this would help underscore the exceptional nature of warrantless powers and ensure that enforcement officers turn their minds to whether it is practicable to obtain a warrant. It would also reinforce the first principle that we have recommended and its underlying premise: that it is desirable for

48 This point was also recently made by the court in *Police v Davies* [2016] DCR 165 at [33] and [35].

49 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.66]–[5.67].

50 A similar fact situation arose in *H v R* [2015] NZCA 49, although there the issue was whether the requirements of s 8 of the Search and Surveillance Act 2012 were satisfied in circumstances where the constable knew the defendant had recently travelled overseas but did not know whether he had returned.

51 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [24]; *R v Laugalis* (1993) 10 CRNZ 350 (CA) at 355–356; *R v H* [1994] 2 NZLR 143 (CA) at 148.

- an independent and impartial person to consider the justification for an intrusion on privacy before it occurs.⁵²
- 4.41 We consider that a general principle of this nature is preferable to a statutory rule that *requires* an enforcement officer to have reasonable grounds to believe that it is impracticable to obtain a warrant before exercising a warrantless power under the Act. Failure to comply with a prescriptive rule requiring a warrant to be obtained in preference to the exercise of warrantless powers would automatically render the exercise of the power unlawful. In contrast, as we have explained in Chapter 3,⁵³ failure to comply with a principle would not—in and of itself—render conduct unlawful or unreasonable.
- 4.42 Instead, the fact that a warrant was readily obtainable would be relevant to an assessment of whether there was an unreasonable search in terms of section 21 of NZBORA. We consider this is appropriate: the availability of a warrant is a factor relevant to reasonableness, not lawfulness. As the case law has recognised, the decision as to whether to exercise a warrantless power will often be influenced by the case-specific realities of policing that are faced by officers at that time. This type of discretionary, evaluative exercise is best reviewed through the rubric of reasonableness rather than a bright line statutory rule.⁵⁴
- 4.43 For completeness, we note that in Chapter 12 we make specific recommendations in relation to sections 110(h) and 125(l) of the Act, which currently give enforcement officers a power to search electronic devices that are located during a search. Sections 110(h) and 125(l) do not, strictly speaking, give enforcement officers “warrantless powers” to search electronic devices. Rather, they are ancillary powers available to officers when exercising search powers (whether under a warrant or warrantless power). As we discuss in that chapter, there is a degree of uncertainty as to whether the warrant preference approach applies to those powers. We make a recommendation to amend those sections to remove the ability for a person executing a warrantless search power under Part 2 of the Act to automatically examine an electronic device, except where there are urgent circumstances.⁵⁵

PRINCIPLE 3: PROPORTIONALITY

- 4.44 The third principle that we recommend is “the principle that State intrusion into an individual’s privacy should be proportionate to the public interest in the investigation and prosecution of the offence or the maintenance of the law”.
- 4.45 Our framing of this principle has drawn on section 21 of NZBORA jurisprudence, particularly the courts’ discussion of the circumstances in which a search may be unreasonable. As Blanchard J explained in *Hamed v R*, once a court has established that there has been a “search”, the second step is to determine whether the search was reasonable in the circumstances.⁵⁶ The courts have repeatedly emphasised that reasonableness is an elastic term⁵⁷ that is not capable of close definition, and can only be assessed in light of the facts and circumstances of a particular

52 As the authors of *The New Zealand Bill of Rights Act: A Commentary* observe, “[a] citizen is substantially prejudiced by a warrantless search: the lack of a warrant document lessens a citizen’s ability to understand the reason for a search and appreciate the limits of what can properly be searched for, and, in addition, means that the comfort that a warrant provides (a neutral third party has approved it, having considered evidence on oath) is not present”: Butler and Butler, above n 21, at [18.18.3].

53 At paragraphs [3.22]–[3.23].

54 That said, we do not consider that s 20 of the Act should be amended to remove the requirement for a constable to believe on reasonable grounds that it is not practicable to obtain a search warrant. In our view, this could have the unintended consequence of suggesting a dilution of the warrant preference approach in relation to s 20 searches.

55 Chapter 12 at paragraphs [12.39]–[12.43].

56 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [172] per Blanchard J.

57 *R v Jefferies* [1994] 1 NZLR 290 (CA) at 304 per Richardson J.

case. For that reason, set categories of “reasonable” activity cannot be formulated.⁵⁸ In *R v Jefferies*, Thomas J described how the question of reasonableness is to be approached:⁵⁹

What is required, to use the language of Dickson J in *Hunter v Southam Inc* (1984) 14 CCC (3d) 97 at p 108, is an assessment as to whether, in the particular situation, the public interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement. ...

- 4.46 In summary, a search will be reasonable where—on the facts and circumstances of the specific case—the public interest in law enforcement outweighs the individual's interest in privacy. The principle we have recommended is intended to reflect this. We have employed the language of “proportionality” because a proportionality inquiry lies at the heart of considering whether limitations on rights and freedoms under NZBORA are justified.⁶⁰
- 4.47 We have also chosen to identify the two factors that need to be balanced against each other, rather than simply stating that the proposed activity should be proportionate to the purpose for which it is to be carried out.⁶¹ This is to make it clear what is being balanced, and also to explicitly recognise the legitimate interest that law enforcement agencies have in the investigation and detection of crime. We have also chosen to refer to the public interest in the investigation and prosecution of “the offence”⁶² (rather than “offending” in general) to make it clear that a case-specific assessment of the particular facts and circumstances is required.
- 4.48 There is an additional point that we need to clarify. We have included a reference to “the maintenance of the law” to accommodate situations where the proposed activity is to be carried out under a declaratory order or in accordance with a policy statement, and the activity is not directed towards the investigation or prosecution of a specific offence. For example, a declaratory order may be sought by enforcement officers in relation to activities they wish to undertake for the purpose of preventing or detecting crime. In that situation, the proposed State intrusion should be proportionate to the public interest in the maintenance of the law. We envisage that a case-specific assessment of the facts and circumstances would also be carried out when conducting this balancing exercise.
- 4.49 As we explained in Chapter 3,⁶³ we see value in a proportionality assessment being carried out formally in advance of the exercise of search and surveillance powers rather than being left for consideration at the “back end”. If an individualised assessment of these considerations is made

58 See *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA) at 405 and 407. See also Paul Rishworth and others *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) at 434; and Scott Optican “Search and Seizure” in Grant Huscroft and Paul Rishworth (eds) *Rights and Freedoms* (Brookers Ltd, Wellington, 1995) 297 at 316 and 323.

59 *R v Jefferies* [1994] 1 NZLR 290 (CA) at 319 per Thomas J. See also *Powerbeat International Ltd v Attorney-General* (1999) 16 CRNZ 562 (HC) at 580–582; *R v Vu* [2013] 3 SCR 657 at [22]; and *R v Ngan* [2007] NZSC 105, [2008] 2 NZLR 48 (SC) at [104], where McGrath J explained that the role of s 21 of the New Zealand Bill of Rights Act 1990 is to regulate State acts involving search and seizure against a yardstick of reasonableness. Therefore application of s 21 “set[s] the point at which privacy rights are limited to accommodate community rights, particularly the public interest in law enforcement, including the detection and prosecution of criminal behaviour”.

60 This is required by s 5 of the New Zealand Bill of Rights Act 1990 (see *Hansen v R* [2007] NZSC 7, [2007] 3 NZLR 1 at [104] per Tipping J); although, as we have noted above at n 30, this consideration is subsumed into the “reasonableness” inquiry when considering potential breaches of s 21 of the Act: see *Cropp v Judicial Committee* [2008] NZSC 46, [2008] 3 NZLR 774 at [33]; and *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [162] per Blanchard J. The authors of *The New Zealand Bill of Rights Act: A Commentary* observe that consideration of the proportionality of the intrusion is “latent within the test discussed in *Hamed*”: Butler and Butler, above n 21, at [18.24.8].

61 Compare s 61(b) of the Intelligence and Security Act 2017.

62 “Offence” includes the plural (see s 33 of the Interpretation Act 1999).

63 At paragraph [3.13].

before a warrant or order is issued or before powers under the Act are exercised, this is likely to reduce the scope for unreasonable searches (under section 21 of NZBORA) to be carried out.⁶⁴

4.50 The courts have also underscored the need for the reasonableness assessment to be made before the search. As Richardson J explained in *R v Jefferies*:⁶⁵

It is implicit in the right to be secure against unreasonable search or seizure that reasonableness is to be assessed *when the search is about to take place* ... The goal is to *prevent* unreasonable searches ...

The assessment of the particular values underlying the right in the particular case and the balancing of those interests against the public interest in the carrying out of the search, have to be made as at the moment the search is to begin. Only in that way is there adequate focus on securing and vindicating individual rights on the one hand and recognising any imperatives of law enforcement on the other.

Disproportionate activity

4.51 In terms of what action an issuing officer or enforcement officer might take, in the event that they consider the proposed State intrusion into privacy is disproportionate to the public interest in the investigation and prosecution of the offence, we consider there are two possible avenues:

- The issuing officer could decide not to issue the warrant or the enforcement officer could decide not to exercise the search power. It is implicit in the wording of section 6 (which states that an issuing officer “may issue a search warrant”) and other provisions that permit issuing officers to issue warrants and orders⁶⁶ that issuing officers have a residual discretion to decline to issue warrants and orders, even if the criteria for their issue are satisfied.⁶⁷
- The issuing officer could add conditions to the warrant,⁶⁸ tailoring the warrant to achieve a fair balance between the public interest in law enforcement on the one hand, and the individual citizen’s rights on the other.⁶⁹

Relevant considerations

4.52 In *Hamed v R*, Blanchard J outlined several considerations that will frequently be taken into account when conducting the reasonableness inquiry, including:⁷⁰

64 As the Law Commission observed in *Search and Surveillance Powers* (NZLC R97, 2007) at [2.55], “it is fundamental to the protection of individual liberty that the need for the exercise of the power should be demonstrated to the satisfaction of an independent officer and authorised by that officer before the exercise of the power rather than justified afterwards with the benefit of hindsight”. The Commission also noted that—even if applications for warrants and orders are almost always approved—the fact that they have to be justified to an independent person is likely to mitigate any risk of abuses or excesses of power: at [2.55]. See also Geoffrey Palmer *A Bill of Rights for New Zealand: A White Paper* (Department of Justice, Wellington, 1985) at [10.156].

65 *R v Jefferies* [1994] 1 NZLR 290 (CA) at 305 per Richardson J (emphasis added). See also *Powerbeat International Ltd v Attorney-General* (1999) 16 CRNZ 562 (HC) at 580–582. See also Crown Law Office *Search and Surveillance Bill (45-1): Consistency with the New Zealand Bill of Rights Act 1990* (12 June 2009) at [11.1].

66 See, for example, ss 53 and 74 of the Search and Surveillance Act 2012.

67 As Fisher J observed in *Television New Zealand Ltd v Police* [1995] 2 NZLR 541 (HC) at 549 (albeit in relation to s 6’s predecessor, s 198 of the Summary Proceedings Act 1957), “[i]n the normal course it can be expected that warrants will be issued whenever the prerequisites have been satisfied but the use of the word ‘may’ imports a discretion. That discretion is well capable of accommodating a consideration of Bill of Rights Act rights and freedoms”. See also *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523 at [117]; *Baron v Canada* [1993] 1 SCR 416, where the Supreme Court of Canada explained that vesting a residual discretion in an authorising judge to decline a search warrant provides an important safeguard, because it prevents “rubber-stamping” of warrants and ensures that the public interest in law enforcement is properly balanced against the individual’s right to be free of intrusions from the State; and Crown Law Office *Search and Surveillance Bill (45-1): Consistency with the New Zealand Bill of Rights Act 1990* (12 June 2009) at [11.2]. Compare, however, *Cullen v District Court at Auckland* [2017] NZHC 465 at [105].

68 A search warrant may be subject to any conditions that the issuing officer considers reasonable: s 103(3)(b) of the Search and Surveillance Act 2012.

69 Butler and Butler, above n 21, at [18.16.11].

70 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [172] per Blanchard J. See also *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA) at 407: “[w]hether a ... search or seizure is unreasonable depends on both the subject-matter and the particular time, place and circumstance”.

- the nature of the place or object that is to be searched;
 - the degree of intrusiveness into the privacy of the persons to be affected; and
 - the reason why the search is occurring.
- 4.53 We envisage that issuing officers and enforcement officers will take those considerations into account when applying the proportionality principle. In relation to the nature of the place or object to be searched, the courts have explained that there is a hierarchy of interests protected by section 21.⁷¹ Accordingly, searches of places or objects in respect of which there is a higher expectation of privacy may require greater justification.
- 4.54 As for the degree of intrusiveness into the privacy of the persons to be affected, we expect that this would require consideration of the size, scope and timing of the proposed search and surveillance activity. Again, more intrusive activities may require greater justification.⁷²
- 4.55 As for the reason why the search is occurring, we expect that consideration would be given to the gravity and extent of the suspected offending. In general, there may be less justification for carrying out a search to target isolated “trivial or truly minor cases” than for more serious suspected offending.⁷³ Similarly, activity carried out for general crime prevention or detection purposes is unlikely to be justified if it involves substantial intrusions on privacy.
- 4.56 We also expect that the proportionality assessment would include consideration of whether the activity can be carried out in a less intrusive manner.⁷⁴ This does not mean, however, that warrants, orders or powers under the Act should only be used “as a last resort”.⁷⁵ The availability of less intrusive means is simply one of a number of factors to be considered when assessing whether the right balance has been struck between the public interest in law enforcement on the one hand, and the individual citizen’s rights on the other. We also note

71 Although the courts have warned against rigid classifications (see *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [114] per William Young P and Glazebrook J), they have observed that, in general: reasonable expectations of privacy are higher within private property than in public places; reasonable expectations of privacy are higher in residential properties than in non-residential properties; reasonable expectations of privacy in the private areas of a residential property, such as drawers or cupboards, are higher than in the front garden, in garages, and in outbuildings; and there is a lesser expectation of privacy in respect of vehicles, commercial premises, and on farmland. See *R v Williams* at [113]–[114]; *R v Jefferies* [1994] 1 NZLR 290 (CA) at 305 per Richardson J; and *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA) at 407. Also, as we discuss in more detail in Chapter 12, the Supreme Courts in New Zealand, Canada and the United States have all recognised that there is generally a high expectation of privacy in respect of the contents of an electronic device: *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [191]; *R v Vu* 2013 SCC 60, [2013] 3 SCR 657; *R v Fearon* 2014 SCC 77, [2014] SCR 621; *Riley v California* 573 US 1 (2014).

72 See *Powerbeat International Ltd v Attorney-General* (1999) 16 CRNZ 562 (HC) at 586, where Hammond J assumed (without deciding) that “the use of powerful techniques may require more justification”. For example, a strip search of an individual may be more intrusive than a rub-down search: see *Forrest v Attorney-General* [2012] NZCA 125, [2012] NZAR 798 at [14]. See also *R v Jefferies* [1994] 1 NZLR 290 (CA) at 305 per Richardson J; and *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [13] per William Young P and Glazebrook J. We note that the Crown Law Office’s advice to the Attorney-General on the Search and Surveillance Bill’s consistency with the New Zealand Bill of Rights Act 1990 recorded that “the greater the degree of intrusiveness, the greater the justification that is required and, further, the greater the attendant safeguards to ensure that that justification is present”: Crown Law Office *Search and Surveillance Bill (45-1): Consistency with the New Zealand Bill of Rights Act 1990* (12 June 2009) at [8].

73 See, for example, *Television New Zealand Ltd v Attorney-General* [1995] 2 NZLR 641 (CA), where the Court of Appeal set out a number of general principles to guide the determination of s 21 reasonableness when the premises of media organisations are searched under warrant. One of those principles was that “the intrusive procedure of a search warrant should not be used for trivial or truly minor cases” (at 647).

74 See also Butler and Butler, above n 21, at [18.24.8] and [18.24.17]. As the authors of *The New Zealand Bill of Rights Act: A Commentary* observe, “[i]n general, where alternative and less intrusive means of acquiring the target information could be provided where those alternatives do not unduly hamper the enforcement agency’s objectives, it is incumbent on those exercising the search powers to use less intrusive means unless further justification be provided”: at [18.24.17].

75 See *R v Rogers Communications Partnership* 2016 ONSC 70 at [61]–[62].

that this factor is already regularly considered under section 30 of the Evidence Act 2006,⁷⁶ and therefore will be familiar to enforcement officers and judges.⁷⁷

PRINCIPLE 4: MINIMISING PRIVACY INTRUSIONS

- 4.57 The fourth principle that we recommend is “the principle that powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected”.
- 4.58 The basis for this recommendation stems, in part, from Chapter 6 of our Issues Paper. In that chapter, we noted that enforcement officers and their assistants can potentially see much more irrelevant material in the course of a digital search than in a physical search,⁷⁸ and we asked submitters whether the Act should be amended to limit the amount of irrelevant material seen during such searches.⁷⁹
- 4.59 We explore this issue in more detail in Chapter 12 of this Report. There, we recommend a number of amendments to the Act that are intended to encourage enforcement officers and their assistants to undertake targeted digital searches. In the course of formulating those recommendations, we considered whether there was an underlying principle that should be extracted and reflected in a principles provision. We came to the view that the need to undertake targeted digital searches represents part of a wider principle that powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any persons likely to be affected. This general principle applies to both digital and non-digital searches.
- 4.60 In our view, this minimal intrusion principle captures two important considerations:
- *The specificity of the warrant:* warrants (and orders) should be as specific as reasonably possible; and
 - *The specificity of the search:* a warrant, order or warrantless power should be executed in a manner that minimises intrusion.
- 4.61 We note that this principle—in some respects—overlaps with the principle of proportionality that we have set out above. For example, a warrant that is overly broad is likely to offend against the principle of minimal intrusion, as well as the principle that State intrusions on privacy should be proportionate to the public interest in the investigation and prosecution of the offence. However, we considered it was appropriate to include a separate reference to the principle of minimal intrusion because the proportionality principle is primarily concerned with whether a warrant or order should be issued at all; whereas the minimal intrusion principle is

76 When considering whether exclusion of improperly obtained evidence is proportionate to the impropriety, the courts may have regard to whether there were any other investigatory techniques not involving any breach of the rights that were known to be available but were not used: s 30(3)(e) of the Evidence Act 2006. See, for example, *Tweeddale v Police* [2015] NZHC 1298 at [51]; and *R v R* [2016] NZCA 200 at [36]. See also *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [272] per McGrath J: “[T]here were no other practicable means [in this case] of effective investigation and monitoring of the emerging situation. That is important to the need for an effective and credible system of justice, which s 30(2)(b) requires be taken into account. If the public concluded that, in future, when a similar situation arose, the police could not effectively investigate it as a crime and be able to gather admissible evidence, strong doubts would reasonably arise over the effectiveness in particular of the justice system”.

77 We initially considered whether consideration of less intrusive means should be included in the principles provision as a stand-alone principle. (There is precedent for this. Section 61 of the Intelligence and Security Act 2017 sets out criteria for the issue of an intelligence warrant. Section 61(b) requires the proposed activity to be proportionate to the purpose for which it is to be carried out; and s 61(c) requires that the purpose of the warrant cannot reasonably be achieved by a less intrusive means.) However, because we consider the principle of proportionality would already require consideration of this factor, we concluded a separate principle was unnecessary.

78 Issues Paper, above n 4, at [6.32]. A “digital search” is a search of stored data (as opposed to data in transit).

79 Question 25.

primarily concerned with whether the terms of a warrant are sufficiently tailored, and whether the search is executed in a reasonable manner.

The specificity of the warrant

4.62 The importance of ensuring that a warrant is as specific as reasonably possible has been emphasised in a number of judicial decisions.⁸⁰ Recently, in *Dotcom v Attorney-General*, a majority of the Supreme Court cited the following passage from *Tranz Rail Ltd v Wellington District Court* with approval:⁸¹

A search warrant is a document evidencing judicial authority to search. That authority must be as specific as the circumstances allow. Anything less would be inconsistent with the privacy considerations inherent in s 21 of [NZBORA]. Both the person executing the warrant, and those whose premises are subject of the search, need to know, with the same reasonable specificity, the metes and bounds of the Judge's authority as evidenced by the warrant ...

4.63 The Court of Appeal in *Tranz Rail* referred to warrants that do not describe the parameters of the warrant, either as to subject-matter or location, with sufficient specificity as “general warrants”, which the courts have confirmed are fundamentally flawed and therefore invalid.⁸²

4.64 The need for a warrant to be as specific as reasonably possible also means that applications for warrants need to be tailored to their purpose. Applications should be as specific as possible⁸³ and should also give issuing officers sufficient information to assess what is necessary and achievable in the particular circumstances.⁸⁴ This is important because it gives the issuing officer the opportunity to impose conditions on the warrant that are designed to minimise the privacy intrusion on persons likely to be affected.⁸⁵

4.65 We note that, in *R v Williams*, the Court of Appeal set out a number of best practice guidelines for search warrant applications.⁸⁶ The Court said that, in general, applications for warrants should adequately describe the offence and specific incident or incidents to which the search relates; sufficiently define the evidential material that the application alleges will be found; and seek authorisation to search only those places where the evidential material is expected to be found.⁸⁷ In other words, the proposed search must be more than “a fishing expedition with nothing in particular in mind”.⁸⁸ *Williams* was a decision that pre-dated the enactment

80 Most recently, see *E v R* [2017] NZCA 222 at [58].

81 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [41], cited in *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 (SC) at [99]. The Court of Appeal also observed that judges who issue warrants that are not as specific as reasonably possible are not balancing the competing interests appropriately: at [42]. See also *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 (SC) at [9] per Elias CJ.

82 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [38], affirming *Auckland Medical Aid Trust v Taylor* [1975] 1 NZLR 728 (CA) at 733. There have been a number of instances where the courts have held that a warrant was overly broad and therefore invalid. See, for example, *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 (CA); *Calver v District Court at Palmerston North (No 1)* [2005] DCR 114, (2004) 21 CRNZ 371; and *F v R* [2015] NZCA 564 at [69] (where the Court held that the warrants in that case were unreasonably vague and general, and therefore fundamentally defective). In *R v Green* HC Auckland CRI-2006-4-16031, 23 November 2007, the High Court held that a warrant granted for a search for class A drugs was overly broad because it included reference to class B and class C drugs, and to manufacturing of methamphetamine, when there was nothing in the application for the warrant supporting those references. In *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523 at [143] the Court expressed some concern that the warrant in that case was too broad. The Court noted that, if there had been proper disclosure of the issues raised by media warrants, conditions could have been designed to better address those concerns.

83 See *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [210] per William Young P and Glazebrook J.

84 See *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 (CA) at [76].

85 By way of example, in *R v Middledorp* [2015] NZHC 1137 at [32], the High Court was critical of an application for a warrant to search for electronic records at the suspects' home, as it did not set out how electronic records were to be obtained, whether anyone would have access to the information before the suspects were informed of the warrant, or what protections there would be for any privileged, private or irrelevant information.

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

87 At [211]–[212] per William Young P and Glazebrook J.

88 At [212] per William Young P and Glazebrook J, referring to *R v Sanders* [1994] 3 NZLR 450 (CA) at 461.

of the Search and Surveillance Act, but in our view, the guidelines set out by the Court are of continuing relevance to applications for warrants and orders under the Act.⁸⁹ They appropriately emphasise that the process of applying for a warrant or order is one-sided in that the issuing officer does not have the benefit of hearing submissions from a defence perspective.

The specificity of the search

4.66 The need to exercise powers under the Act in a manner that involves minimal intrusion reflects the fact that searches must be conducted in a reasonable manner. A search that is carried out unreasonably exceeds the authority conferred by the warrant or statutory power.⁹⁰ As the Supreme Court of Canada explained in *R v Vu*:⁹¹

[A]n authorized search must be conducted in a reasonable manner. *This ensures that the search is no more intrusive than is reasonably necessary to achieve its objectives.* In short, prior authorization prevents unjustified intrusions while the requirement that the search be conducted reasonably limits potential abuse of the authorization to search.

4.67 The courts have, on a number of occasions, emphasised the need for searches to be executed in a minimally intrusive manner. In *R v Ririnui* the Court of Appeal observed that “[t]he intrusiveness and invasion of privacy involved in any search of the person is such that it ought to be conducted to no greater extent than the circumstances reasonably require”.⁹² In *R v Briggs*, the Court stated that an unannounced peaceable entry of occupied residential premises or a forced entry of occupied residential premises without prior refusal was likely to be unreasonable.⁹³ And in *R v Hapakuku*, the Court criticised a decision to execute a search warrant at a person’s home in the middle of the night.⁹⁴

4.68 We expect that, in general, a search will be no more intrusive than is necessary where it is conducted so as to cause the least practicable disruption to the person or persons affected.⁹⁵ (This may include persons who are not the suspects or targets of the search or surveillance activity.) In the context of digital searches, we envisage that this principle will encourage enforcement officers and their assistants to plan and conduct targeted searches. This is discussed further in Chapter 12.

PRINCIPLE 5: TE AO MĀORI AND CULTURAL, SPIRITUAL OR RELIGIOUS CONSIDERATIONS

4.69 The fifth principle that we recommend is “the principle that powers under the Act should be exercised having regard to te ao Māori and any other relevant cultural, spiritual or religious considerations”.

4.70 The basis for this recommendation stems, in part, from a submission we received from Te Hunga Rōia Māori o Aotearoa, who suggested that the Act ought to include a specific

89 This was also the approach adopted by the Court of Appeal in *F v R* [2015] NZCA 564 at [76].

90 *Simpson v Attorney-General [Baigent’s Case]* [1994] 3 NZLR 667 (CA) at 694. See also *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [46] per William Young P and Glazebrook J (the search must be “lawful, not unreasonably executed and not [extending] further than to fulfil the lawful purpose”); and *Television New Zealand Ltd v Police* [1995] 2 NZLR 541 (HC) at 549–550.

91 *R v Vu* [2013] 3 SCR 657 at [22] per Cromwell J (emphasis added).

92 *R v Ririnui* [1994] 2 NZLR 439 (CA) at 442.

93 *R v Briggs* [1995] 1 NZLR 196 (CA) at 202.

94 *R v Hapakuku* (1999) 16 CRNZ 520 (CA) at 525. See also *R v Pratt* [1994] 3 NZLR 21 (CA) at 24, where a strip search conducted in a public street in the middle of the day was lawful but unreasonable because it was executed at a time and place that disregarded the dignity of the person who was searched; and *Frost v Police* [1996] 2 NZLR 716 (HC) at 725, where a warrantless search of a person for evidence of drugs was held to be unreasonable because the use of police dogs to assist in the search was an excessive use of force in the circumstances.

95 See, for example, *Television New Zealand Ltd v Attorney-General* [1995] 2 NZLR 641 (CA), where the Court observed that media search warrants should be executed “considerately and so as to cause the least practicable disruption to the business of the media organisation” (at 648).

reference to the Treaty of Waitangi/te Tiriti o Waitangi (the Treaty). Te Hunga Rōia submitted this could be achieved either by:

- amending section 5(b) of the Act to state that one of the purposes of the Act is to “provid[e] rules that recognise the importance of the rights and entitlements affirmed in te Tiriti o Waitangi and other enactments, including the New Zealand Bill of Rights Act 1990, the Privacy Act 1993 and the Evidence Act 2006”; or
- inserting a separate provision into the Act that states that the Treaty must be taken into account when exercising powers under the Act.

4.71 Te Hunga Rōia submitted that it was important for legislation to include references to the Treaty where relevant, because of its constitutional role as the founding document of New Zealand. It also submitted that Māori have a particularly strong interest in search and surveillance legislation because they are disproportionately represented within the criminal justice system and also have particular relationships with the whenua (land).

References to the Treaty of Waitangi in statute

4.72 The Treaty of Waitangi has been described as “part of the fabric of New Zealand society”⁹⁶ and is undoubtedly of significant constitutional importance.⁹⁷

4.73 The author of *Burrows and Carter Statute Law in New Zealand* observes that, over time, the Treaty has become increasingly relevant to statute law.⁹⁸ First, it is now well-established that the New Zealand courts will presume that Parliament intends to legislate in accordance with the principles of the Treaty, even where it is not mentioned in the text of the legislation.⁹⁹

4.74 Second, New Zealand statutes often make express reference to the Treaty. These provisions vary in the recognition accorded to the Treaty and the effect that the Treaty has on the statute as a whole.¹⁰⁰ For example, some statutes indicate in their long titles, preambles or in purpose or principles provisions that the Act’s purpose is to recognise or give effect to the principles of the Treaty.¹⁰¹ Others require officials to act consistently with the Treaty.¹⁰² Legislation may refer to the Treaty for a number of different reasons, for example, in order to:¹⁰³

... facilitate resolution of claims under the Treaty; secure rights protected by the Treaty; mandate consideration of the Treaty or Treaty principles; mandate consideration of Māori interests or the role of Māori as tangata whenua; promote equal employment opportunities for Māori; acknowledge cultural differences; promote Māori language or culture, or use of Māori land; or implement Treaty settlements.

4.75 In a 2014 report, *Regulatory Institutions and Practices*, the New Zealand Productivity Commission identified 36 statutes that contain references to the Treaty or Treaty principles.¹⁰⁴

96 *Huakina Development Trust v Waikato Valley Authority* [1987] 2 NZLR 188 (HC) at 210.

97 See *New Zealand Maori Council v Attorney-General* [1994] 1 NZLR 513 (PC) at 516 per Lord Woolf.

98 Ross Carter *Burrows and Carter Statute Law in New Zealand* (5th ed, online ed, LexisNexis, Wellington, 2015) at 520–525.

99 See, for example, *Takamore v Clarke* [2011] NZCA 587, [2012] 1 NZLR 573 (CA) at [248], *Huakina Development Trust v Waikato Valley Authority* [1987] 2 NZLR 188 (HC) at 223 and *Barton-Prescott v Director-General of Social Welfare* [1997] 3 NZLR 179 (HC) at 184. This presumption of consistency derives support from the Legislation Design and Advisory Committee Guidelines, which suggest that all proposed legislation is examined with regard to its Treaty implications at the policy approval stage: *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) ch 4. See also the Cabinet Office *Cabinet Manual 2017* at [7.65].

100 *Laws of New Zealand – Treaty of Waitangi* (online looseleaf ed, LexisNexis) at [142].

101 See, for example, the Environment Act 1986 (preamble) and Te Ture Whenua Maori Act 1993 (preamble).

102 See, for example, the Hazardous Substances and New Organisms Act 1996, s 8; Resource Management Act 1991, s 8; and State-Owned Enterprises Act 1986, s 9.

103 Philip Joseph *Constitutional and Administrative Law in New Zealand* (4th ed, Brookers Ltd, Wellington, 2014) at [4.9.4(2)].

104 New Zealand Productivity Commission *Regulatory Institutions and Practices* (June 2014) at [7.3].

The Commission noted that “[t]here appears to have been a trend towards the inclusion of more specific Treaty clauses that specify the action to be taken in satisfaction of Treaty principles instead of broadly stated Treaty clauses, in more recent legislation”.¹⁰⁵

- 4.76 The Productivity Commission considered that considerable care was required when deciding the circumstances when legislation should include reference to Treaty principles. This was because:¹⁰⁶

By including a Treaty clause in statute, it will be clear that legal provision is being made for Māori rights. It also signals the Crown’s intent, compared to the absence of such a clause. But the nature and magnitude and implications of those rights may not be clear to the regulator, Māori, other stakeholders, and even the courts.

- 4.77 The Productivity Commission suggested that the decision to include a Treaty clause in legislation should be made on a case-by-case basis. It suggested a number of factors to be considered when making that decision, such as whether Māori have a strong, relatively unified and legitimate interest in the policy being developed; whether Māori would have the capacity to effectively litigate to protect their rights; and the degree of uncertainty likely to be generated for stakeholders.¹⁰⁷

Our recommendation

- 4.78 We have considered whether it is appropriate to include a Treaty clause in the Search and Surveillance Act.¹⁰⁸ We have concluded that it is not, primarily because we are concerned that a Treaty clause would generate uncertainty for enforcement officers around the nature and scope of their powers under the Act, and the action they need to take in order to satisfy their Treaty obligations, particularly in relation to consultation.
- 4.79 We note that Te Hunga Rōia suggested that a Treaty clause could be supplemented by more detailed clauses that specify the action to be taken: for example, the Act could include a provision requiring enforcement officers (before exercising search and surveillance powers) to seek advice on Māori privacy interests from a specially constituted panel of tikanga experts. While we can see merit in such a process being followed in some cases, our preference is for the Act to provide enforcement agencies with sufficient flexibility to develop their own protocols (which may involve general and/or case-specific consultation with Māori) on how to execute search and surveillance powers in a culturally sensitive manner. Requiring consultation with a panel in all cases would likely cause significant delay and prejudice effective law enforcement.
- 4.80 We therefore consider that the Act should specifically recognise Māori interests in a general principle that “powers under the Act should be exercised having regard to te ao Māori and any other relevant cultural, spiritual or religious considerations”. We consider that this principle will direct issuing and enforcement officers’ minds to the need to carry out search and

105 At [7.3]. See similarly *Burrows and Carter*, above n 98, at 531.

106 At [7.6].

107 At [7.6]. The Commission also noted that—if a decision was made that including a Treaty clause was appropriate—the next step would be to decide on the *form* of that clause (for example, whether it is specific or broad): at [7.6].

108 We note that we have not considered the more general question of whether references to the Treaty and its principles ought to be included—as a matter of course—in New Zealand statutes. In our view, that question raises broader issues about the exact constitutional role of the Treaty within New Zealand law, consideration of which is best-placed within the context of any future review of our constitutional arrangements. See, for example, the observations in Matthew Palmer “The Treaty of Waitangi in Legislation” [2001] NZLJ 207 at 212: “If a generic reference to the Treaty in a particular statute is still necessary to protect the minority Maori interest, then it must be necessary in all statutes and should therefore be a generic provision residing in the Constitution Act 1986 or Interpretation Act 1999. This requires a more general, informed, constitutional debate than we have had to date on these issues”. See more generally Matthew Palmer *The Treaty of Waitangi in New Zealand’s Law and Constitution* (Victoria University Press, Wellington, 2008); and more recently, Geoffrey Palmer and Andrew Butler *A Constitution for Aotearoa New Zealand* (Victoria University Press, Wellington, 2016) ch 7 and He Whakaaro Here Whakaumu Mō Aotearoa *The Report of Matike Mai Aotearoa, The Independent Working Group on Constitutional Transformation* (2016).

surveillance powers in a culturally sensitive manner. The express reference to te ao Māori is intended to recognise the special relationship between the Crown and Māori in New Zealand.¹⁰⁹ The reference to other cultural, spiritual or religious considerations recognises that respect for the practices of all cultures and religions is important in our increasingly multicultural society.¹¹⁰

- 4.81 In our view, this principle is consistent with the existence of section 5(b) of the Act (which states that one of the purposes of the Act is to provide rules that recognise the importance of the rights in NZBORA) and sections 13, 15 and 20 of NZBORA (which enshrine the right to freedom of religion and belief, the right to manifest that religion or belief, and the rights of minorities).
- 4.82 However, unlike the other principles we have discussed, this principle has not been the subject of direct consideration in New Zealand case law in the search and surveillance context.¹¹¹ We therefore do not have the benefit of judicial consideration of its practical application. In addition, we acknowledge that te ao Māori is a broad concept that is open to different interpretations. The principles in the Act should provide meaningful guidance to enforcement officers and issuing officers, not create uncertainty. Accordingly, further work may be required to refine the wording of the principle.
- 4.83 The principle is intended to encourage the execution of search and surveillance powers in a culturally sensitive manner, where it is clear that cultural, spiritual or religious considerations are likely to arise (for example, where an enforcement agency intends to search a church or mosque). In taking the principle into account, we envisage enforcement agencies may consult with relevant groups in advance of developing any relevant internal guidance or policy statements and/or on a case-by-case basis. For example, if an enforcement agency intended to execute a search warrant in relation to land that has special significance to Māori (such as a marae or an urupā), consultation with Māori may assist the agency in carrying out the search in a respectful manner.¹¹²
- 4.84 We do not consider that inclusion of this principle will unduly hinder law enforcement activities. That is because Police, for example, already has existing internal protocols on executing searches in culturally sensitive circumstances. Under these protocols, officers are expected to complete a “community impact assessment” if there is any concern that an issue of cultural sensitivity might arise. The reports require the officer to consider what the adverse impacts of a search might be in advance of its execution. Further, where appropriate, officers are expected to consult with others (for example, iwi liaison officers)¹¹³ in order to develop a plan for how to execute the search in a way that would eliminate or minimise the negative effects of the operation.

109 We also note that the Act already appears to anticipate that Māori customs and practices will be respected during the exercise of search and surveillance powers. For example, when exercising search powers under the Act, s 110(b) authorises the person exercising the power to request assistance with the entry and search from a member of a hapū or an iwi, if the place to be entered is of cultural or spiritual significance to that hapū or iwi. See similarly s 117(1)(b) and the reference to marae in s 342 of the Search and Surveillance Act 2012.

110 See Statistics New Zealand *2013 QuickStats about culture and identity* (April 2014) at 6–7 and 27–29; and Superu *Families and Whānau Status Report 2016* (July 2016) at 79. Also, as we noted in Chapter 2, individuals from different cultural backgrounds may have differing perceptions of privacy.

111 In a more general context, see *Takamore v Clarke* [2012] NZSC 116, [2013] 2 NZLR 733 at [164] per Tipping, McGrath and Blanchard JJ (“the common law of New Zealand requires reference to ... tikanga, along with other important cultural, spiritual and religious values”). See also at [94] and [101] per Elias CJ.

112 For example, by having regard to the specific kawa (protocol) of a marae.

113 Iwi liaison officers are part of Police (either police officers or police employees). Their role is to help navigate cultural issues and to work on improving police relationships with Māori.

PRINCIPLE 6: MINIMISING IMPACT ON CHILDREN AND VULNERABLE PEOPLE

- 4.85 The sixth principle that we recommend is “the principle that powers under the Act should be exercised in a manner that minimises the impact on children and vulnerable members of the community”. We use the phrase “vulnerable members of the community” to include the elderly, people with physical, intellectual, psychological or psychiatric impairments,¹¹⁴ people with medical needs, and people who are not fluent in English (for example, people for whom English is a second language). There is existing case law on the meaning of “vulnerable” that would provide further guidance.¹¹⁵
- 4.86 This principle was suggested to us by the Human Rights Commission and is allied to the minimal intrusion principle that we have recommended above (principle 4). That principle is reflected in case law and requires powers under the Act to be executed in a minimally intrusive manner. We expect application of that principle would, in general, mean that searches are executed in a considerate manner and so as to cause the least practicable disruption to children and vulnerable members of the community.¹¹⁶
- 4.87 However, we see value in including a specific principle in the Act designed to minimise the negative impact on children and vulnerable people. We agree with the view expressed to us by the Human Rights Commission that it is important to highlight the special interests of these individuals and ensure that close consideration is given to how they may be adversely affected by search and surveillance activity in any given case.¹¹⁷
- 4.88 Again, we do not expect that recognition of this principle will be unduly burdensome for enforcement officers. We note, for example, that Police already has existing internal protocols on how searches that impact on children and vulnerable people are to be executed. Police officers are expected to consider how any negative impacts can be eliminated or minimised. This might include, for example: making inquiries for an appropriate caregiver to be present at the search to care for children, young people or the elderly; ensuring that a search is executed during the daytime rather than at night; and ensuring that someone who can speak the language of those affected by the search is present.

PRINCIPLE 7: PRIVILEGE

- 4.89 The final principle that we recommend is “the principle that powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any individual”.
- 4.90 The basis for this recommendation stems from a suggestion by the Human Rights Commission as well as Chapters 6 and 8 of our Issues Paper, where we asked submitters whether the Act adequately protects privileged material during the exercise of search or surveillance powers.¹¹⁸

114 See similarly s 103(3)(b) of the Evidence Act 2006.

115 See, for example, the case law concerning s 9(1)(g) of the Sentencing Act 2002 (which recognises offending against a particularly vulnerable victim as an aggravating factor in sentencing). That case law is discussed in Simon France (ed) *Adams on Criminal Law – Sentencing* (online looseleaf ed, Thomson Reuters) at [SA9.12].

116 Like principle 5, we acknowledge that New Zealand case law in the search and surveillance context has not directly addressed the importance of minimising privacy intrusions on children and vulnerable people. However, in our view, it is implicit in the well-established case law on minimising privacy intrusions (which we set out above at paragraphs [4.66]–[4.68]) that application of that principle would involve minimal disruption to children and vulnerable people.

117 We also note that, although there is no stand-alone right to privacy in the New Zealand Bill of Rights Act 1990, New Zealand ratified the United Nations Convention on the Rights of the Child 1577 UNTS 3 (opened for signature 20 November 1989, entered into force 2 September 1990) in 1993, which affirms that everyone under the age of 18 years has the right to privacy (art 16).

118 Issues Paper, above n 4, questions 24, 25 and 35.

One of the issues we identified with the Act is that it does not require any application under it to identify any privilege issues of which the applicant is reasonably aware.¹¹⁹

- 4.91 We suggested that the protection of privileged material could be strengthened by requiring privilege issues to be addressed in applications for warrants or orders under the Act. We noted this would be consistent with the duty of candour, which is well-established under the common law.
- 4.92 The importance of the duty of candour was emphasised by the Court of Appeal in *Tranz Rail Ltd v Wellington District Court*.¹²⁰ The Court explained that—because an application for a search warrant is almost always made on an *ex parte* basis¹²¹—the issuing officer to whom the application is made “is entitled to expect that the applicant will make full and candid disclosure of all facts and circumstances relevant to the question whether the warrant should be issued”.¹²² A failure to make such disclosure runs the risk that any warrant obtained will be held to be invalid.¹²³
- 4.93 More recently, in *Hager v Attorney-General*, Clifford J discussed the role of a judge when considering and granting an application for a search warrant. His Honour observed:¹²⁴

If nothing else, where such a warrant is applied for, the judge should be satisfied not only that the police are themselves aware of [privilege] 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.

Submissions

- 4.94 The majority of submissions we received on this issue were in favour of the Act requiring applications for warrants or orders to identify any privilege issues of which the applicant is reasonably aware. They submitted that an express statutory duty would be consistent with the common law duty of candour, and would provide greater clarity and certainty for enforcement agencies.
- 4.95 Also relevant are the submissions we received on the issue of whether the Act adequately protects privileged material from being seen by enforcement agencies during digital searches.¹²⁵ We received four submissions that considered the Act adequately protected such material. One of those submitters considered that this was achieved through section 145, which requires a person conducting a search to provide a reasonable opportunity for a claim to privilege to be made if they come across material that may be privileged. We also received a submission that considered that the courts’ application of section 21 of NZBORA had adequately confirmed the obligations on enforcement agencies to ensure that warrants contain protections for privileged material.

119 At [8.33]–[8.45].

120 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA).

121 That is, without notice to the party whose premises are to be the subject of the proposed search.

122 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [21], referring to *R v McColl* (1999) 17 CRNZ 136 (CA) at 142–143.

123 At [21]. The Court went on to say that “[t]he judicial officer, when deciding whether to issue the warrant, is an important part of a judicial process which is designed to strike the right balance between the interests of the applicant and those of the party to be searched”: at [22], referring to *R v Burns (Darryl)* [2002] 1 NZLR 204 (CA) at 209. The Supreme Court confirmed the ongoing relevance of *Tranz Rail* since the enactment of the Search and Surveillance Act in *Beckham v R* [2015] NZSC 98, [2016] 1 NZLR 505 at [127].

124 *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523 at [117].

125 Issues Paper, above n 4, question 24.

- 4.96 In contrast, four submitters considered the Act did not provide enough protection for privileged material during the execution of digital searches. One of those submitters considered that the Act's protection of privilege was somewhat retrospective and that more proactive protection of privilege was needed. Another submitter considered the Act did not sufficiently protect privileged material from being seen during either a digital or non-digital search.

Our recommendation

- 4.97 Our view is that applications for warrants and orders should adequately signal when issues of privilege may arise and contain sufficient information to enable issuing officers to determine whether the procedures in the Act for managing privilege are adequate or whether further conditions need to be imposed.
- 4.98 To give effect to this proposal, we recommend that the Act is amended to require enforcement officers exercising powers under the Act and issuing officers to take into account the principle that powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any person. We use the word “privilege” to refer to the privileges that are recognised under the Act¹²⁶ and the rights conferred on journalists under section 68 of the Evidence Act 2006 to protect their sources.¹²⁷
- 4.99 We have suggested the inclusion of this general principle rather than the insertion of a specific statutory rule requiring applications to identify privilege issues. This recognises that the Act is designed to protect privileged material throughout the investigation phase (including during the actual execution of the search), not solely at the application phase. (For example, as noted above, where a person is executing a search warrant or exercising a search power and forms reasonable grounds to believe that anything discovered during the search may be the subject of privilege, the Act requires them to provide the person who might be able to claim privilege with a reasonable opportunity to do so.¹²⁸)
- 4.100 We considered whether—in addition to a general principle—there should be an express requirement for an enforcement officer to include information about any privilege issues of which they are aware in an application for a warrant or order. We concluded there should not be such a requirement. This is because, as we explained in Chapter 3,¹²⁹ the principles we have recommended contain several matters in respect of which supporting information could be provided in an application for a warrant or order: for example, information relating to the impact on third parties (principle 4) and information relating to cultural sensitivities (principle 5). We do not want to suggest there is a hierarchy amongst the principles by only expressly requiring privilege issues to be identified in applications.

126 These are set out in s 136 of the Search and Surveillance Act 2012.

127 See s 136(1)(i) of the Search and Surveillance Act 2012.

128 Section 145.

129 At paragraphs [3.29]–[3.30].

RECOMMENDATION

- R5 The principles section should provide that:
- (a) enforcement officers and issuing officers must take into account the principle that conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement;
 - (b) enforcement officers exercising powers under the Act must take into account the principle that a warrant or order should be obtained in preference to exercising a warrantless power;
 - (c) issuing officers and enforcement officers exercising powers under the Act must take into account the principles that:
 - (i) State intrusion into an individual's privacy should be proportionate to the public interest in the investigation and prosecution of the offence or the maintenance of the law;
 - (ii) powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected;
 - (iii) powers under the Act should be exercised having regard to te ao Māori and any other relevant cultural, spiritual or religious considerations;
 - (iv) powers under the Act should be exercised in a manner that minimises the impact on children and vulnerable members of the community; and
 - (v) powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any individual.

Chapter 5

Policy statements

INTRODUCTION

- 5.1 During our review, we identified a number of areas where we think greater guidance for enforcement officers would be beneficial to ensure that search and surveillance activity is carried out in a reasonable manner. Statutory rules cannot cover every eventuality, and some discretion and flexibility needs to be retained to enable effective law enforcement. However, there are risks in leaving too much discretion to enforcement officers without providing sufficient guidance on how the law applies in particular contexts.
- 5.2 In this chapter, we recommend that chief executives of enforcement agencies be required to issue policy statements in relation to a number of types of search and surveillance activity. These policy statements would be made publicly available to promote transparency and accountability in enforcement agencies' practices.
- 5.3 This chapter covers matters that would be common to all policy statements, such as their intended effect and the process for issuing them. It does not explain the rationale for requiring a policy statement in each particular context or discuss the type of guidance that should be included in each policy statement. Those issues are discussed in later chapters, because the approach will vary depending on the subject matter.

BACKGROUND

Issues Paper

- 5.4 The recommendations in this chapter developed out of the discussion in our Issues Paper about public surveillance.¹ We referred to the fact that some surveillance in public places or using publicly available information—such as the use of CCTV cameras² or social media monitoring³—is generally lawful without any statutory authorisation because it does not involve trespass or the commission of an offence. However, these lawful techniques still have the potential to intrude on reasonable expectations of privacy, depending on how they are carried out and how the information gathered is used.
- 5.5 We suggested that there might be merit in the Search and Surveillance Act 2012 (the Act) regulating some public surveillance activities. However, because public surveillance is often used on an ongoing basis for general crime prevention and detection purposes rather than to investigate a specific offence, we thought a warrant regime was unlikely to be appropriate. We suggested that statutory criteria or a policy statement might better reflect the ongoing and generally lawful nature of the activity, and create less of a compliance burden for enforcement agencies.

1 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.104]–[3.109].

2 Closed-Circuit Television (CCTV) is a self-contained surveillance system comprising cameras, recorders and displays for monitoring activities in public or on private premises.

3 “Social media” refers to internet-based communication platforms that enable users to share information (including messages, videos, pictures and any other content). Examples include Facebook, Twitter, Instagram, web forums and blogs. “Social media monitoring” refers to enforcement officers accessing social media platforms to obtain information about individuals or classes of individuals.

- 5.6 We discuss issues relating to public surveillance and the submissions we received on that topic in more detail in Chapter 11. For present purposes, it is sufficient to note that we formed the view warrants should not be required but further guidance on the use of some public surveillance methods would be beneficial. The surveillance methods we discuss can be conducted without breaching the law but may still intrude on reasonable expectations of privacy. Guidance would help to ensure that any such intrusion is reasonable, so will not breach section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA).
- 5.7 The principles we have recommended in Chapter 4 will assist in this regard. However, in relation to methods that are not subject to specific statutory powers or authorisation mechanisms, it will not necessarily be clear to enforcement officers or the public when those principles are engaged or how they should be applied. We reached the view that requiring policy statements to be issued for certain classes of activity would be an appropriate way of providing greater guidance to enforcement officers without unduly hampering enforcement activity that is generally lawful.
- 5.8 While our proposal to introduce policy statements arose in the context of public surveillance, we subsequently identified several other areas where we thought their use would be beneficial. These are areas where some relevant statutory provisions exist (or where we recommend they be introduced) but further guidance is desirable on activity falling outside their scope, or on whether or how those provisions apply in particular contexts.⁴
- 5.9 A similar mechanism already exists in the Act for strip searches. Section 126 requires chief executives of enforcement agencies whose officers may carry out strip searches to issue guidelines on the circumstances under which such searches can be conducted. In addition, policy statements have been introduced in relation to the activities of the New Zealand Security Intelligence Service (NZSIS) and Government Communications Security Bureau (GCSB) under the Intelligence and Security Act 2017.⁵ That Act requires ministerial policy statements to be issued for a range of lawful activities, including surveillance in public places.⁶

Consultation

- 5.10 We discussed the concept of policy statements with our Officials Group and Expert Advisory Group. Most officials did not see the need for formal statements, preferring to have internal guidance where they consider that is appropriate. They emphasised the need for agencies to determine the content of their own policies, as another person or body is unlikely to have a sufficient understanding of their operational context. Some were also concerned that being required to publish statements might disclose sensitive operational information that could prejudice their investigations.
- 5.11 Our Expert Advisory Group was more supportive of requiring policy statements to be issued. While there was a general preference for statutory rules rather than guidelines, most experts acknowledged rules will not be appropriate in some contexts (such as public surveillance) given the shades of grey involved in determining what amounts to an intrusion on reasonable expectations of privacy. They considered that requiring policy statements to be published would be an improvement on the status quo, particularly in areas where developments in technology increase the potential intrusion involved in lawful methods of surveillance.

⁴ As we discuss below at paragraphs [5.21]–[5.25], this includes guidance on interception and tracking with consent, when production orders should be obtained, and the circumstances and manner in which covert operations should be conducted.

⁵ Intelligence and Security Act 2017, ss 206–216.

⁶ Section 206(e).

PURPOSE OF POLICY STATEMENTS

- 5.12 The aim of the ministerial policy statement regime in the Intelligence and Security Act 2017 is to provide a greater level of oversight and accountability for the activities for which a policy statement is required; and to help ensure compliance with the law by providing guidance to the NZSIS and GCSB on any grey areas where it may be unclear whether a particular type of activity is lawful or appropriate in the absence of a warrant.⁷ We envisage policy statements would fulfil a similar function in the Search and Surveillance Act.
- 5.13 Policy statements would provide guidance on the use of methods that are lawful – either because they are permitted under the general law, or because they have been authorised under the Act. They would set out the appropriate procedures to be followed and considerations to be taken into account to help ensure the relevant method is only used in appropriate cases and in a reasonable manner. They may also indicate situations in which a warrant or order under the Act (or other legislation) ought to be obtained or when an activity risks becoming unlawful or unreasonable.
- 5.14 Policy statements would need to reflect, and be consistent with, the principles of the Act and any relevant legislation or case law (for example, the Privacy Act 1993 will be relevant in the context of public surveillance). They would provide context-specific guidance on how those principles and requirements apply to particular types of activity.
- 5.15 We consider this guidance will be valuable for enforcement officers, who will have a clearer idea of the steps they need to take to make sure they are acting lawfully and reasonably. This, in turn, may help to reduce subsequent challenges to the admissibility of evidence in subsequent proceedings and claims against the Crown for breaches of NZBORA. Policy statements will also help to achieve greater consistency in practices between government agencies. They will provide a mechanism for agencies to become aware of how the law is interpreted and applied by other agencies and to reach a common position.
- 5.16 As we discuss below, policy statements would need to be made publicly available (with the exception of any information that could be withheld under the Official Information Act 1982). In this way, they would increase the transparency of law enforcement activity. In turn, this will allow the public to engage with questions about when intrusions into privacy are justified; and enhance the accountability of enforcement agencies. Members of the public would be able to raise concerns if they consider that practices outlined in the statement are inappropriate or that an enforcement agency has not complied with an applicable statement – for example, by complaining to the Independent Police Conduct Authority (IPCA)⁸ or the relevant Minister or campaigning for law changes to make it clear that certain practices are not permissible.

EFFECT OF POLICY STATEMENTS

- 5.17 Policy statements would be similar to a code of conduct or code of practice. They would give guidance on best practice. Enforcement officers would be required to have regard to policy statements when carrying out any activity to which they apply.
- 5.18 The fact that an enforcement officer has disregarded or acted inconsistently with a policy statement could influence a court's assessment of whether they have acted unreasonably (for

⁷ Sir Michael Cullen and Dame Patsy Reddy *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (Wellington, 2016) at [6.66].

⁸ The Independent Police Conduct Authority can investigate complaints about Police practices, policies or procedures that affect the person or body of persons making the complaint (Independent Police Conduct Authority Act 1988, s 12(1)(a)(ii)).

the purposes of section 21 of NZBORA) and whether evidence obtained should be excluded in subsequent proceedings.⁹ However, it would not in itself make an act unlawful or unreasonable.

- 5.19 Policy statements would not be legislative instruments or disallowable instruments.¹⁰ They could not render lawful an activity that would otherwise be unlawful; or make an unreasonable search reasonable.

ACTIVITY THAT SHOULD BE COVERED BY POLICY STATEMENTS

- 5.20 We have concluded that the following types of public surveillance should require a policy statement:

- the use of visual surveillance technology in circumstances not requiring a surveillance warrant (“public visual surveillance”);
- accessing social media platforms to obtain information about individuals or classes of individuals (“social media monitoring”);
- observation or monitoring of an individual’s movements or activities in a manner not requiring a surveillance warrant (“directed surveillance”).¹¹

We set out the reasons why we consider policy statements are appropriate in those instances in Chapter 11.

- 5.21 In addition to public surveillance, there are five other areas where we consider policy statements should be required. First, in Chapter 9, we recommend that the exception from the requirement to obtain a warrant for interception where one party consents should be retained. However, given the potential for such interception to intrude on the privacy of the other party, we recommend a policy statement be issued in relation to interception with consent. The policy statement would also apply to tracking with consent.
- 5.22 Second, in Chapter 14, we recommend policy statements should be issued in relation to production orders. We discuss the current uncertainty about when an enforcement officer needs to apply for a production order rather than seeking voluntary disclosure of information from a service provider.¹² Issues were also raised with us about the level of specificity of production orders. We have concluded that it would not be plausible to set out detailed statutory criteria on when a production order must be obtained. However, we think further guidance—in the form of a policy statement—would increase certainty and transparency about the circumstances and manner in which enforcement agencies can obtain information from third parties (such as service providers).

9 Under s 30 of the Evidence Act 2006, one of the factors to be taken into account in determining whether to exclude improperly obtained evidence is whether the impropriety was deliberate, reckless or done in bad faith (s 30(3)(b)).

10 Legislative instruments are laws made by the Governor-General, Ministers of the Crown, and certain other bodies under powers conferred by an Act of Parliament. Common examples include regulations and rules. The statutory definition encompasses most Orders in Council, instruments made by a Minister that amend an Act or define the meaning of a term used in an Act, instruments required to be published under the Legislation Act 2012 and some resolutions of the House of Representatives (Legislation Act 2012, s 4). Disallowable instruments include legislative instruments and some other, non-legislative instruments (Legislation Act 2012, s 38). They must be presented to the House of Representatives, which can disallow the instrument with the consequence that it ceases to have effect (Legislation Act 2012, ss 41–44).

11 For example, following a person in a car or tracking a fleeing offender from a helicopter.

12 We use the term “service provider” to refer to private sector businesses that provide a service to customers. This includes telecommunications network operators, internet service providers, banks, electricity and gas suppliers and transport companies.

- 5.23 Third, in Chapter 15, we recommend that warrants should be available under the Act for covert operations (more commonly known to the public as undercover operations).¹³ However, warrants would not be required in most cases. Even where a warrant is obtained, we consider general guidance on the manner in which covert operations should be conducted would be beneficial in light of their complexity and potentially high level of intrusiveness. We consider that a policy statement could usefully set out the principles and procedures that need to be applied whenever covert operations are being considered or carried out.
- 5.24 Fourth, in Chapter 15, we also recommend that a statutory regime be introduced in the Act permitting New Zealand Police (and possibly some other enforcement agencies) to obtain and use assumed identities – for example, obtaining passports under false names for use by undercover officers. A policy statement should also be issued providing guidance on the acquisition and use of assumed identities. This is similar to the approach taken in the Intelligence and Security Act.¹⁴
- 5.25 Fifth, the current requirement in section 126 of the Act for chief executives to issue guidelines on strip searches appears to fulfil a similar function to what we would envisage policy statements performing. Policy statements would also be issued (as we discuss below) by chief executives. In the interests of simplicity and consistency, we recommend that the guidelines requirement be replaced with a requirement to issue a policy statement.
- 5.26 In addition to these specific areas, we think the Act should allow additional policy statements to be issued. This may be useful where a particular type of activity is generally lawful but has the potential to intrude on reasonable expectations of privacy (and therefore amount to a “search” in terms of section 21 of NZBORA). For example, we envisage new policy statements might be issued where technologies develop that enable surveillance in public places (or in relation to publicly available information) that does not fall within one of the specific types of public surveillance we are recommending policy statements be required for.
- 5.27 We only make recommendations in this chapter about two types of policy statements discussed above (strip searches and additional statements). The other types of policy statements we have referred to are discussed in greater detail later in this Report, so our recommendations relating to those statements appear in the relevant chapters.¹⁵

PROCESS FOR ISSUING POLICY STATEMENTS

Who should issue policy statements?

- 5.28 We were initially attracted to the idea of requiring policy statements to be issued by Ministers. That is the approach taken in the Intelligence and Security Act. Ministerial approval would help to achieve a level of independence from the day-to-day operational realities of enforcement agencies. It would also allow for more direct accountability if the public disagree with the approach taken in a statement, since Ministers are elected Members of Parliament.
- 5.29 However, ministerial approval would cause difficulty where Police activity is concerned. By constitutional convention, reflected in the Policing Act 2008 and case law, the Commissioner of Police must act independently from the Government of the day when making decisions about

13 As we explain in Chapter 15 at paragraphs [15.1], [15.13]–[15.14] and [15.96], the term “covert operations” encompasses a wider range of activity than traditional undercover operations. We use it to refer to any situation where an enforcement officer (or another person acting at the direction of an enforcement agency) interacts with another person for the purpose of obtaining access to information on the basis of deception – for example, by obscuring their true identity or the fact the information will be provided to Police.

14 Intelligence and Security Act 2017, ss 21–32 and 206(b)–(c).

15 See chapters 9 (interception and tracking), 11 (public surveillance), 14 (production orders) and 15 (covert operations and assumed identities).

the enforcement of the criminal law in particular areas or types of cases.¹⁶ It is possible that policy statements would provide some guidance on such operational matters (for example, they might indicate that the use of a particular technique will only be appropriate where a certain type of offending is being investigated). We would not wish to restrict the matters that could be covered in policy statements by requiring them to be issued by Ministers. We therefore recommend that the Commissioner of Police should issue policy statements relating to Police.

- 5.30 We considered whether policy statements relating to non-Police enforcement agencies should be issued by Ministers, since the same difficulties do not arise. However, we saw potential problems with requiring Commissioner approval of Police policy statements and ministerial approval of others. We wish to encourage co-ordination of statements between enforcement agencies to ensure consistent practices are adopted across government where appropriate. In some areas, joint statements or model statements adapted for specific agencies might be appropriate. This is likely to be difficult if Ministers issued some statements, as the Commissioner of Police's independence may be compromised if the Commissioner was required to consult them.
- 5.31 On balance, we consider that policy statements should be issued by the chief executive of the relevant agency. In addition to making consultation and co-ordination between agencies easier, approval by chief executives will make the approval process quicker and less resource-intensive for agencies. Although chief executives are not elected, they could still be subject to complaints or media pressure if the public is concerned about the approach taken in a policy statement. In the case of non-Police agencies—and potentially Police in some cases, depending on the issue involved—Ministers could choose to intervene.
- 5.32 The function of issuing policy statements should be non-delegable to ensure a sufficiently high level of scrutiny.

Consultation

- 5.33 Since policy statements would be drafted and approved within the relevant enforcement agency, we consider that some external scrutiny is appropriate. We propose that the Commissioner of Police or the relevant chief executive should be required, before issuing a statement, to consult the Ministry of Justice, the Privacy Commissioner and any other person or organisation they consider appropriate. We would expect this to include any government agencies with an interest in the subject-matter. In addition to other relevant enforcement agencies, consultation with NZSIS and GCSB is likely to be appropriate in some cases (for example, in relation to the policy statements on the acquisition and use of assumed identities).¹⁷ These consultation requirements will help ensure statements:
- are consistent with the Act (which the Ministry of Justice administers), including its principles;
 - are consistent with the Privacy Act 1993;
 - have appropriate regard to the privacy implications of the activities covered by the statement; and

16 Policing Act 2008, ss 16 and 30(4)(a); *LP v Attorney-General* [2016] NZAR 511 (HC) at [12]–[15]; *Evers v Attorney-General* [2000] NZAR 372 (HC).

17 As we discuss in Chapter 15, the assumed identity regime we recommend including in the Act would be similar to the one in the Intelligence and Security Act 2017. Some alignment between the policies issued by enforcement agencies and those issued by NZSIS and GCSB may therefore be desirable.

- are consistent with policy statements already published or being prepared by other agencies, to the extent appropriate.

5.34 In addition, consultation with the Ministry of Justice will assist the Ministry to identify areas where the Act is unclear or ineffective. It can then brief the Minister of Justice and suggest amendments to the Act as appropriate.

5.35 Chief executives would be required to have regard to any feedback provided by consultees but would not be obliged to amend the statement. If a consultee had concerns about the approach ultimately adopted, they would be free to raise those concerns publicly, with Ministers, or—in the case of Police—with the IPCA.

Publication

5.36 Policy statements would need to be made publicly available on the enforcement agency's website and in any other manner the chief executive considers appropriate. Specific information could be omitted from the published statements if there would be grounds for withholding it under the Official Information Act 1982.¹⁸ This should address the concern expressed by some enforcement agencies that publishing policy statements might prejudice future investigations.¹⁹

Duration

5.37 Each policy statement would be valid for five years. Before the expiry of that term, the statement would need to be revised and a replacement issued. Policy statements could be revised more frequently if required (for example, if changes in technology mean that new guidance is desirable).

5.38 We do not make a recommendation about the date by which the first policy statements must be issued. If our proposals to require policy statements are adopted, the Ministry of Justice would need to consult enforcement agencies to determine a realistic timeframe. Our initial view is that a period of one year from the date of enactment of any amendment Act ought to be adequate.

RECOMMENDATIONS

- R6 Provisions should be inserted into the Act to require policy statements:
- (a) to be issued in respect of specified classes of activity undertaken by enforcement agencies and in relation to any other class of activity the issuer considers appropriate; and
 - (b) to be consistent with the principles in the Act, the Privacy Act 1993 and any other applicable legislation or case law.
- R7 The Act should require enforcement officers to have regard to policy statements when carrying out any activity to which they apply.
- R8 The current requirement in section 126 for chief executives to issue guidelines on strip searches should be replaced with a requirement to issue a policy statement on strip searches.

¹⁸ Official Information Act 1982, ss 6 and 9.

¹⁹ One of the grounds for withholding information is if disclosure would “prejudice the maintenance of the law, including the prevention, investigation, and detection of offences” (Official Information Act 1982, s 6(c)).

- R9 Policy statements relating to Police should be issued by the Commissioner of Police. Policy statements relating to other enforcement agencies should be issued by the chief executive of the relevant agency. The function of issuing policy statements should be non-delegable.
- R10 Before issuing a policy statement, the Commissioner of Police or the chief executive of the relevant agency should be required to consult the Ministry of Justice, the Privacy Commissioner and any other person or organisation they consider appropriate and to have regard to any feedback received.
- R11 Policy statements should be published on the Police or relevant agency's website and in any other manner the Commissioner or chief executive considers appropriate. Information should, however, be able to be omitted from a policy statement if there would be grounds for withholding it under the Official Information Act 1982.
- R12 Each policy statement should be valid for a maximum of five years.

Chapter 6

Declaratory orders

INTRODUCTION

- 6.1 In our Issues Paper, we identified some possible problems with the declaratory order regime in the Search and Surveillance Act 2012 (the Act). These problems are in part exemplified by the fact that, to the best of our knowledge, only one declaratory order has so far been obtained.¹ We asked for submitters' views on whether declaratory orders should be replaced with a residual warrant regime.
- 6.2 In this chapter, we explain why we have concluded that a residual warrant regime would be inappropriate and that the declaratory order regime should be retained. We discuss concerns that were raised with us about the propriety of judges making declaratory orders. Those concerns are based on the Act's description of the orders as being "advisory" in character, which, as we explain, we consider is not the case. We recommend some amendments to the declaratory order provisions to clarify the purpose and effect of the orders.

BACKGROUND

The statutory scheme

- 6.3 Under the Act, an enforcement officer can apply for a declaratory order if they wish to use a device, technique or procedure, or carry out an activity that:²
- is not specifically authorised by another statutory regime; and
 - may constitute an intrusion into the reasonable expectation of privacy of any other person.
- 6.4 Only judges (as opposed to any issuing officer) can make declaratory orders.³ The orders are described in section 65(1) as follows:
- A declaratory order is a statement by a judge that he or she is satisfied that the use of a device, technique, or procedure, or the carrying out of an activity, specified in the order is, in the circumstances of the use or the carrying out of the activity specified in the order, reasonable and lawful.
- 6.5 The Act states that the orders are "advisory in character" and do not affect the ability of subsequent courts to determine whether the specified activity was reasonable and lawful.⁴ However, the Act does provide immunity from civil and criminal liability for any act done in good faith that is covered by a declaratory order.⁵ This means that individual enforcement officers or their assistants are not penalised for acting in reliance on a declaratory order.
- 6.6 The only condition that must be met in order for a declaratory order to be issued is that the judge be satisfied that the specified activity, *in the circumstances of its proposed use*, is reasonable

1 New Zealand Police *Annual Report 2015/2016* at 152. That order related to the use of drug detection dogs at consenting domestic courier depots.

2 Search and Surveillance Act 2012, s 66.

3 Section 68. "Judge" is defined as either a High Court or District Court judge (s 3).

4 Section 65(2).

5 Section 165(b).

and lawful.⁶ The order must describe the device, technique, procedure or activity that it relates to; the person, place, vehicle or other thing that is the object of its use (if available); the circumstances in which the use or activity will be undertaken; and the purpose of the use or activity.⁷

- 6.7 Several observations can be made about these provisions. First, orders can only be issued in relation to use or activity that the judge considers to be reasonable and lawful. This means the orders—unlike search warrants and surveillance device warrants—cannot authorise unlawful activity such as trespass or unauthorised access to a computer system.⁸ They also cannot legitimise activity that would amount to an unreasonable search or seizure in terms of section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA), although the fact a declaratory order was obtained might influence a court’s assessment of whether the evidence gathered should be admitted in subsequent proceedings.⁹
- 6.8 Second, the grounds for issuing a declaratory order are broad. Unlike other warrants and orders under the Act, the judge does not need to be satisfied that there are reasonable grounds to believe an offence has been committed, or reasonable grounds to suspect evidential material will be obtained. This means that declaratory orders can be sought by enforcement officers in relation to activities they wish to undertake for the purpose of preventing or detecting crime (rather than just investigating specific offences).
- 6.9 Third, the orders must specify the circumstances in which the use or activity is to be undertaken and its purpose. The object of the use or activity must also be identified where possible. This is very similar to the information that must be included in a surveillance device warrant.¹⁰ These requirements mean that declaratory orders cannot authorise the general use of a new technology or investigatory technique. If the enforcement agency wishes to use the same technology or technique again, it will require a new declaratory order. Declaratory orders are therefore similar to other warrants and orders under the Act in the sense that they are context-specific.
- 6.10 Finally, the orders are expressly stated to be advisory and not binding on a court considering the lawfulness and reasonableness of the activity after it has occurred. This has created some debate about the appropriateness of judges issuing advisory orders, as we discuss further below.¹¹

Legislative history

- 6.11 The Law Commission’s 2007 Report, *Search and Surveillance Powers*, recommended that the Act include a residual warrant regime.¹² This regime would have required enforcement officers to obtain a residual warrant in order to use a device that interfered with reasonable expectations of privacy but was not otherwise subject to regulation. Residual warrants would have been issued by a judge on the same grounds as a surveillance device warrant.

6 Section 68.

7 Section 69.

8 Crimes Act 1961, s 252.

9 Under s 30(3)(b) of the Evidence Act 2006, one of the relevant considerations is whether the impropriety was “deliberate, reckless, or done in bad faith”. It seems unlikely such a finding would be made where a declaratory order has been obtained.

10 See s 55(3)–(4) of the Search and Surveillance Act 2012. Under s 55(4), a surveillance device warrant need not specify the object of the surveillance or the evidential material that will be obtained if that information is unavailable. Instead, the warrant can specify “the circumstances in which the surveillance is to be undertaken in enough detail to identify the parameters of, and objectives to be achieved by, the use of the surveillance device”.

11 See paragraphs [6.18] and [6.26].

12 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) recommendation 11.24.

- 6.12 The Commission considered that such a regime was desirable because the specific warrants it recommended including in the Act would not cover all eventualities.¹³ The surveillance device warrant regime would only cover the use of interception, tracking and visual surveillance devices in certain situations. The Act would not specifically address the use of other surveillance devices or surveillance not using a device.
- 6.13 The Commission thought a residual regime would reinforce the rule of law and the “presumptive requirement that all search, seizure, interception and surveillance activity be conducted pursuant to warrant”.¹⁴ It would help to ensure consistency with human rights, provide a measure of certainty to enforcement agencies and reduce challenges to law enforcement activity in subsequent criminal trials.
- 6.14 As introduced, the Search and Surveillance Bill 2009 largely reflected the Commission’s recommendation.¹⁵ However, during the Select Committee process submitters expressed concern that judges would be able to authorise any kind of surveillance technique without any defined limits.¹⁶ Some submitters thought that each new surveillance technique needed to be individually considered and regulated, rather than being dealt with through a general regime.¹⁷
- 6.15 In response to these submissions, the Ministry of Justice and the Law Commission advised in the departmental report that:
310. ... The intent of the regime is not to make lawful the use of new devices, techniques, or procedures that are otherwise unlawful. Indeed, it is intended that an order will be issued only in relation to devices, techniques, or procedures that are already lawful and reasonable.
311. In summary, the regime is intended to provide an enforcement officer with a measure of comfort that evidential material obtained through a new technique or procedure, or use of a new device is unlikely later to be found to be unreasonable under section 21 of NZBORA.
312. The current drafting does not reflect this intention. The use of the term “warrant” suggests that it authorises enforcement officers to do something that they would otherwise be unable to do. Likewise, the regime’s provisions mirror those of the surveillance device warrant regime when these two regimes are quantitatively different.
313. The residual warrant regime should be recast as a “declaratory order” regime. The regime will make it clear that a declaratory order does not authorise an activity, technique or device that would otherwise be unlawful or unreasonable. The order merely provides judicial clarification that the activity, technique, or device is currently lawful and reasonable.
- 6.16 This suggestion resulted in the Bill being amended to replace residual warrants with declaratory orders.¹⁸ The Hon Judith Collins, then Minister of Justice, clarified that these orders would allow for judicial consideration of the reasonableness of a new device or activity, but could not permit trespass.¹⁹
- 6.17 While the residual warrant regime had shared many similarities to the other warrants in the Bill, the declaratory order provisions were changed substantially. The “reasonable grounds” threshold applying to search warrants²⁰ was removed, in favour of a much broader inquiry as to

13 At [11.121].

14 At [11.131].

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

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

17 At [307].

18 Search and Surveillance Bill 2009 (45-2) (select committee report) at 14 and cls 57–61.

19 (20 March 2012) 678 NZPD 1100.

20 See s 6 of the Search and Surveillance Act 2012.

whether the proposed activity is lawful and reasonable. Many of the procedural requirements that the residual warrant regime shared with search warrants and surveillance device warrants were also removed. For example, as enacted, the declaratory order regime does not apply the search warrant provisions that allow an issuing officer to require more information from the applicant and require the applicant to confirm the truth and accuracy of the application.²¹ We have been unable to find any explanation for these changes.

- 6.18 The new declaratory order provisions received some criticism from opposition Members of Parliament. This included the following arguments:²²
- The “advisory” nature of the orders is inconsistent with the doctrine of separation of powers. It is not for judges to provide opinions to the executive. That should be done by the Crown Law Office.
 - The value of the orders would be limited since they would not be able to authorise trespass.
 - Although the orders would not be binding on a later court, they may place a subsequent court in a difficult position (for example, if in a District Court case the judge is asked to depart from a declaratory order issued by a High Court judge).

CONSULTATION

Issues Paper

- 6.19 In our Issues Paper, we identified some problems with how the declaratory order regime is operating in practice:²³
- because the orders are only “advisory” and do not bind a later court, they do not give enforcement officers a high degree of certainty that they are acting lawfully; and
 - the extent to which the orders help to future-proof the legislation is limited, since they cannot authorise any activity that amounts to a trespass or is otherwise unlawful.
- 6.20 However, we also noted that the limited nature of the declaratory order regime provides a relatively high degree of rights protection. It means that Parliament must expressly consider whether to amend the Act to permit the use of novel techniques that would, if not authorised, breach the law.²⁴
- 6.21 We sought submitters’ views on whether the declaratory order regime should be replaced with a residual warrant regime similar to the one originally recommended by the Law Commission. This would allow judges to authorise any search or surveillance activity not covered by a specific statutory regime, provided certain criteria were met.²⁵ Unlike declaratory orders, residual warrants would be able to permit activity involving trespass or some other breach of the law (in a similar way to search warrants and surveillance device warrants).
- 6.22 We considered the primary benefit of this approach was that it would allow the legislation to respond to technological developments without requiring constant amendment. Enforcement agencies would be able to use the most effective and efficient tools available to them, subject to a judge being satisfied that certain criteria were met.

21 Search and Surveillance Act 2012, ss 98(2) and 99. Other relevant procedural requirements are set out in ss 100, 101 and 105. These provisions are all applied to surveillance device warrants by ss 52(2) and 58.

22 (7 March 2012) 678 NZPD 971 and (20 March 2012) 678 NZPD 1095 per Charles Chauvel MP and Hon David Parker MP.

23 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [2.79]–[2.80].

24 At [2.86].

25 At [2.89]–[2.101].

Submissions

- 6.23 The majority of submitters who expressed a view on this issue supported replacing declaratory orders with a residual warrant regime. They thought this would increase the flexibility of the Act to deal with new developments and provide greater legal certainty.
- 6.24 However, some submitters who supported a residual regime did so only on the basis that it would be mandatory: that is, the Act would require enforcement officers to obtain a residual warrant before carrying out any activity that would invade a reasonable expectation of privacy. This would significantly increase the level of oversight of enforcement activity and protection of rights. Only four submitters—all enforcement agencies and prosecutors—expressly favoured a residual regime without a mandatory warrant requirement.
- 6.25 The submitters who opposed a residual warrant regime (including the Human Rights Commission) argued that:
- the legislature, not judges, should make policy decisions about whether the use of new, unlawful techniques is justified;
 - residual warrants would allow surveillance powers to be broadened to a potentially limitless degree; and
 - if new surveillance methods are not specifically regulated by statute, it will be more difficult to legally challenge them.
- 6.26 We also received comments from judges of the senior courts²⁶ opposing such a regime. They considered that legislation conferring intrusive powers should be prescriptive rather than conferring broad discretion on issuing officers. They also opposed the retention of the declaratory order regime currently in the Act. The judges' concern was that the orders, being "advisory" in nature, involve the judiciary in a determination that is for the executive to make. They also thought that prospective approval of enforcement activity may result in subsequent litigation about the extent of disclosure made to the issuing officer.

THE CASE AGAINST RESIDUAL WARRANTS

- 6.27 As is evident from our Issues Paper, we initially saw some appeal in a residual warrant regime. We considered it would increase the flexibility of the Act and its ability to respond to changes in technology, avoiding the need for constant amendments. However, after further consideration, we are now of the view that such a regime would be inappropriate.
- 6.28 At its heart, this issue is about who should be able to authorise the use of new investigatory methods that would otherwise breach the law. We think that Parliament should consider whether the use of a new technique that would otherwise be unlawful is justified and, if so, what protections should be placed on its use. These are policy rather than legal questions. We think it is appropriate that they be determined by elected representatives rather than judges, particularly in light of the high public interest in surveillance and its potential impact on human rights. The legislative process provides greater transparency than the issue of a warrant (as warrants, unlike judgments of a court, are not generally available to the public) and allows for public input into the decision-making process.
- 6.29 We are also concerned that a residual warrant regime would not allow for different types of investigatory techniques to be subject to different thresholds or criteria. The Act currently places greater restrictions on the use of some types of surveillance than others. For example,

26 The senior courts are the High Court, Court of Appeal and Supreme Court (see the Senior Courts Act 2016).

interception and visual trespass surveillance can only be carried out in relation to offences punishable by at least seven years' imprisonment (or certain other specified offences).²⁷ This restriction was put in place on the recommendation of the Select Committee that considered the Search and Surveillance Bill. The Committee thought these types of surveillance were particularly intrusive and should be more tightly circumscribed.²⁸

- 6.30 Equally, new technologies or investigatory methods may vary in their levels of intrusiveness. Parliament may consider it appropriate to impose greater restrictions on some (for example, through higher offence thresholds or by limiting which enforcement officers can apply for a particular type of warrant). A residual warrant regime would necessarily treat all methods the same, since its purpose would be to address the use of techniques that are not specifically contemplated by legislation. Specific legislative provisions would ensure a more consistent approach based on a position reached after significant political debate and public consultation. We therefore consider that the dangers of a broad generic approach in the search and surveillance context outweigh the potential benefits.²⁹
- 6.31 Aside from allowing greater flexibility to deal with new technology, submitters who supported a residual warrant regime thought it would provide greater certainty for enforcement officers than the current declaratory order regime. However, as one submitter and a number of enforcement agency representatives pointed out to us, warrants do not have precedent value. Issuing officers do not publish judgments when they determine warrant applications. That means another issuing officer is unlikely to know if similar circumstances have been dealt with previously.
- 6.32 Equally, in a subsequent prosecution, warrants are no more binding on courts than declaratory orders. Warrants are frequently challenged—in some cases successfully—on the basis that they were improperly issued or executed in an unreasonable manner.³⁰
- 6.33 We are therefore not convinced that residual warrants would provide greater certainty than declaratory orders. We also think that much of the uncertainty surrounding declaratory orders can be removed by making some minor amendments to clarify their effect, as we discuss below.³¹

RETAINING THE DECLARATORY ORDER REGIME

- 6.34 The next question is whether the declaratory order regime should be retained. We understand that a declaratory order has so far only been sought (and issued) on one occasion,³² which calls into question the utility of the orders.
- 6.35 As we have noted above, judges of the senior courts have expressed concern that the issuing of advisory opinions to the executive is inconsistent with the judicial role.³³ This mirrors the concerns raised by opposition Members of Parliament during the passage of the Bill.³⁴

27 Search and Surveillance Act 2012, s 45.

28 Search and Surveillance Bill 2009 (45-2) (select committee report) at 4.

29 See the discussion in Paul Ohm "The Argument against Technology-Neutral Surveillance Laws" (2010) 88 Tex L Rev 1685 at 1686.

30 See, for example, *R v C* [2016] NZHC 2935 (upheld in *C v R* [2017] NZCA 154); *Murray and Yates v R* [2016] NZCA 221; and *F v R* [2015] NZCA 564.

31 See paragraphs [6.70]–[6.82].

32 New Zealand Police *Annual Report 2015/2016* at 152. That order related to the use of drug detection dogs at consenting domestic courier depots.

33 See paragraph [6.26].

34 See paragraph [6.18].

- 6.36 We explain below why we think there is value in the declaratory order regime such that it should be retained. We also address the lack of use of the orders to date and the concern that the issuing of declaratory orders is inconsistent with the judicial role.

The value of declaratory orders

- 6.37 We consider that declaratory orders have the potential to be a valuable tool if enforcement agencies gain more confidence in using them. Because the orders cannot authorise unlawful activity, they cannot expand the scope of surveillance powers. As such, they do not give rise to the same concerns as residual warrants about judges usurping the role of Parliament. The orders simply provide a mechanism for enforcement agencies to test the justification for an activity that may intrude on reasonable expectations of privacy with an independent and impartial person.
- 6.38 We think such a mechanism, if it is used more often, will help to prevent unreasonable searches from occurring and foster public trust and confidence in the justice system. As we have discussed in Chapter 2, the courts' ability to exclude improperly obtained evidence in subsequent proceedings cannot perform this kind of preventative or fostering function.³⁵ Review by the courts after the event does little to protect rights and is incomplete as a remedy for breaches of rights.³⁶ By contrast, a declaratory order—like a warrant—places a judicial officer “between the police and the citizen” to assess the justification for an intrusion on privacy before it occurs.³⁷ To use the words of Hammond J in *R v Williams*:³⁸

The rights of citizens to be free from unjustifiable government intrusion are predicted [sic] on a system of prior authorisation, not subsequent validation. And there must inevitably be elements of caprice, uncertainty, and variation in the balancing process between citizen and state where the enforcement authorities are themselves permitted a large licence to conduct warrantless searches.

- 6.39 With the rapid development of technology, opportunities for State intrusion into the lives of individuals are many and varied. Intrusion can occur without the State engaging in unlawful conduct; hence, section 21 of NZBORA protects against unreasonable search and seizure.
- 6.40 We see the retention of the declaratory order regime as necessary to help give effect to the principle that conduct that may constitute an intrusion into the reasonable expectations of privacy of any person should be carried out pursuant to a warrant, order, statutory power or policy statement. This principle would be unable to operate effectively if the Act did not enable enforcement officers to seek authorisation where no specific warrant, provision or policy statement applies.
- 6.41 While the Act would, under our proposals, enable new policy statements to be issued,³⁹ that will take some time. In addition, statements will not anticipate every situation. There will always be grey areas where the lawfulness or reasonableness of a proposed activity is unclear. If authorisation is unavailable in these cases, enforcement officers will be left with the uncomfortable choice of either doing nothing—risking losing evidence or failing to protect the public—or proceeding on the basis of an internal assessment that the proposed course of action is likely to be lawful and reasonable. In our view, that is undesirable.

35 Section 30 of the Evidence Act 2006. See Chapter 2 at paragraphs [2.70]–[2.72].

36 Because this assessment only occurs after the event, it does not prevent breaches of rights from occurring. Although the prospect of evidence being excluded may deter enforcement officers from risking unreasonable searches, we note that evidence is often admitted under s 30 even if it is found to have been improperly obtained. See paragraph [2.70] and n 147 in Chapter 2.

37 See *Parker v Churchill* (1985) 9 FCR 316 (FCA) at 322 per Burchett J, cited with approval by Hammond J in *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [269].

38 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [270].

39 See Chapter 5.

Increasing the uptake of declaratory orders

- 6.42 Declaratory orders can only protect against unreasonable searches occurring if enforcement officers seek them more regularly. The principles we have recommended will encourage their greater use.⁴⁰ However, it will also be necessary to address (so far as possible) any problems that are currently preventing their use.
- 6.43 From our discussions with enforcement agencies, it appears the orders have been underutilised partly because enforcement officers are not familiar with them. Enforcement officers are also unsure about the effect of the orders, which makes them hesitant to use the regime. They expressed some uncertainty about whether the orders are confined to a specific use of a device or technique, or whether they can provide a general authorisation. They also doubted whether the orders could safely be relied upon since they are not binding on a later court.
- 6.44 As we have explained, in our view, the Act makes it clear that declaratory orders must relate to a specific set of facts.⁴¹ They cannot authorise the general use of a new device or technique. As we discussed in Chapter 5, policy statements will be able to provide guidance of more general application. However, we see a continued role for declaratory orders in providing case-specific assessments.
- 6.45 As to the concern that declaratory orders are not binding on a later court, we have already explained above that warrants are no different in this respect.⁴² That does not mean that they have no value. They provide an assessment of the proposed conduct that is detached from the enforcement imperatives of the executive branch of government. As such, they should provide greater assurance—both to enforcement officers and members of the public—than an internal legal opinion. In our view, the same can be said of declaratory orders.
- 6.46 We also note that both warrants and declaratory orders confer immunities on persons acting in reliance on them (provided they act in good faith).⁴³ So, while obtaining a warrant or order does not entirely remove the risk that evidence will be excluded in later proceedings, individual enforcement officers are not at risk of prosecution.
- 6.47 We would therefore encourage enforcement agencies to seek declaratory orders in more cases rather than relying solely on internal advice about the legality and reasonableness of conduct that might intrude on reasonable expectations of privacy.⁴⁴ We make some recommendations below that we hope will clarify the effect of the orders and make them more accessible.⁴⁵

The role of judges in making declaratory orders

- 6.48 We now turn to the concern expressed by judges of the senior courts that the issuing of declaratory orders amounts to giving advisory opinions to the executive and is inconsistent with the judicial role. We think these concerns in large part stem from a lack of clarity about the purpose and effect of the orders. In particular, the use of the term “declaratory order” (which

40 See Chapter 4. The first principle, discussed at [4.6]–[4.27], is that conduct that may constitute an intrusion into the reasonable expectations of privacy of any person should be carried out pursuant to a warrant, order, statutory power or policy statement. This should encourage the use of the declaratory order regime where there is no specific warrant, order, statutory power or policy statement that applies.

41 See paragraphs [6.6] and [6.9].

42 See paragraph [6.31].

43 Search and Surveillance Act 2012, s 165.

44 At present, our understanding is that most activity that could be covered by a declaratory order either proceeds on the basis of an assessment by the enforcement agency (occasionally with the assistance of Crown Law Office advice) that it is lawful and reasonable; or does not proceed at all because there is significant uncertainty about whether it is permissible.

45 See paragraphs [6.70]–[6.82].

suggests a parallel to orders under the Declaratory Judgments Act 1908)⁴⁶ and the reference in subsection 65(2) to the orders being “advisory in character” are problematic. They suggest that the task a court is being asked to undertake is substantively different from the warrant process.

- 6.49 As we explain below, we do not think that is the case. Declaratory orders are much like a warrant except that they do not authorise unlawful activity. They are not “advisory” in the sense that term has been used in case law; they must relate to defined circumstances. In our view, the power to issue declaratory orders is consistent with the judicial role, although some amendments would clarify the position.

Declaratory orders are not “advisory opinions”

- 6.50 The courts frequently express reluctance to issue advisory opinions. This concern often surfaces where a declaration is sought under the Declaratory Judgments Act,⁴⁷ but it can also arise in other situations.⁴⁸ We set out below how “advisory opinions” are characterised in the case law and why they are of concern to the judiciary. The purpose of this discussion is to illustrate why, in our view, declaratory orders under the Search and Surveillance Act do not raise the same problems.

- 6.51 The term “advisory” is used in case law to refer to situations where the court is asked to make a declaration about the meaning of a statutory provision or legal instrument “in a vacuum” or in the abstract.⁴⁹ In these cases the declaration sought will have no practical effect on the rights of the parties.⁵⁰ The concern is not simply that the declaration sought relates to the legality of acts that have not yet occurred. Both the Declaratory Judgments Act and case law confirm that declarations can be made in relation to intended future actions.⁵¹ Rather, a decision is “advisory” where there is no specific fact situation that the court is being asked to consider⁵² or the scenario presented is entirely hypothetical.⁵³

- 6.52 Asher J explained the concern surrounding advisory opinions in *Simpson v Whakatane District Court (No 2)*:⁵⁴

It is a well recognised common law principle that it is contrary to public policy for the Courts to entertain proceedings where there is no actual outstanding issue in existence between the parties. The Courts are not, in general terms, available to provide a free or subsidised opinion service to the

46 Declaratory orders under the Search and Surveillance Act do share some similarities with orders under the Declaratory Judgments Act 1908, which may be why that term was used. Orders can be made under s 3 of the Declaratory Judgments Act to determine a question about the construction of a statute where it will affect the validity of a proposed action. However, orders under the Declaratory Judgments Act are made following argument from both sides and are binding on all of the parties (ss 4 and 5). By contrast, declaratory orders under the Search and Surveillance Act are made on an ex parte application (that is, without the target of the activity being notified or represented) and are not binding on a later court. They also relate exclusively to activity by enforcement agencies, whereas anyone can seek a declaratory order under the Declaratory Judgments Act.

47 *Matamu v Si'itia* [2016] NZHC 2516 at [71]; *Canterbury Regional Council v Attorney-General* [2009] NZAR 611 (HC) at [22]; *Auckland City Council v Taubmans (New Zealand) Ltd* [1993] 3 NZLR 361 (HC) at 365.

48 *Independent Fisheries Ltd v Minister for Canterbury Earthquake Recovery [Leave to Appeal]* [2013] NZSC 35, 2 NZLR 397 at [7]; *R v Gordon-Smith (on appeal from R v King)* [2008] NZSC 56, [2009] 1 NZLR 721 at [25]; *Wellington City Council v McBride* [2006] DCR 452 (HC) at [29].

49 *Auckland City Council v Taubmans (New Zealand) Ltd* [1993] 3 NZLR 361 (HC) at 365 per Barker J.

50 *R v Gordon-Smith (on appeal from R v King)* [2008] NZSC 56, [2009] 1 NZLR 721 at [16]; *Te Whakakitenga O Waikato Inc v Martin* [2016] NZCA 548, [2017] NZAR 173 at [39]; *Hutchinson v A* [2015] NZCA 214, [2015] NZAR 1273 at [11].

51 Declaratory Judgments Act 1908, s 3; *Mandic v Cornwall Park Trust Board* [2011] NZSC 135, [2012] 2 NZLR 194 at [8] and [82]; *Auckland City Council v Taubmans (New Zealand) Ltd* [1993] 3 NZLR 361 (HC) at 365; *Proprietors of Hiruharama Ponui Block Inc v Attorney-General* [2003] 2 NZLR 478 (HC).

52 See *R v Gordon-Smith (on appeal from R v King)* [2008] NZSC 56, [2009] 1 NZLR 721 at [25].

53 *Omaha Beach Residents' Society Inc v Townsend Brooker Ltd* [2010] NZCA 413, [2011] NZRMA 1 at [46].

54 *Simpson v Whakatane District Court (No 2)* [2006] NZAR 247 (HC) at [22]. His Honour also expressed concern that if there is no active dispute, a decision may be made without all available arguments and material being put before the Court. This concern arises in the context of declaratory judgments because they are binding (Declaratory Judgments Act 1908, s 4). The court has no opportunity to reconsider its decision if further relevant facts or arguments come to light at a later point in time. By contrast, declaratory orders under the Search and Surveillance Act are not binding on a later court (Search and Surveillance Act 2012, s 65(2)). The legality and reasonableness of the activity concerned can be challenged after the event.

public. Court time is a precious commodity, and cannot sensibly be spent on deciding matters that only have academic interest, or which prove a point of opinion rather than resolve a dispute.

- 6.53 For example, in *Independent Fisheries Ltd v Minister for Canterbury Earthquake Recovery*, the Supreme Court declined leave to appeal in a case where the applicants had successfully had the Minister’s decisions about land use in greater Christchurch set aside.⁵⁵ The applicants were not challenging the outcome of the Court of Appeal’s decision but rather the reasons for it. There was no longer any live factual dispute between the parties. The “decision” sought would amount to an advisory opinion on the Minister’s powers and how they should be exercised in future cases.⁵⁶
- 6.54 Similarly, in *Omaha Beach Residents’ Society Inc v Townsend Brooker Ltd*, the Court of Appeal declined to make a declaration about the enforceability of a restrictive covenant on the basis that the issue was hypothetical.⁵⁷ The declaration was sought in contemplation of a future application for resource consent or plan change. The Court had no information about the nature of the application or whether it would affect the respondents’ lots, nor did it know whether the respondents would seek to enforce the covenant if they were affected.
- 6.55 As we have explained, declaratory orders under the Search and Surveillance Act must—like a warrant—relate to specific facts. They cannot be made in the abstract. Applications for declaratory orders, and the orders themselves, must identify the proposed activity; the object of the activity (if available); the purpose of the activity; and the circumstances in which the activity will be carried out.⁵⁸ If an application does not spell out with sufficient clarity what the enforcement officer proposes to do and the surrounding circumstances, it would not meet these statutory requirements and the order would not be granted.⁵⁹
- 6.56 Furthermore, while declaratory orders do not relate to a live “dispute” between two parties, they do have a practical effect on the actions of enforcement officers. We therefore do not consider declaratory orders can properly be described as “advisory” in character if they meet the statutory requirements.
- 6.57 We also note that the Supreme Court has accepted it may be appropriate to answer a “general question in relation to future conduct” where it is of significant public importance.⁶⁰ That will be particularly likely where the case involves a public authority and raises a question of public law.⁶¹ To the extent that there is any residual concern about declaratory orders being “advisory” in character, we consider that they may well satisfy these criteria. They concern the extent to which public authorities can legitimately intrude on the privacy interests of individuals, which is a matter of considerable public interest.

Issuing declaratory orders is consistent with the judicial role

- 6.58 The primary function of the courts is to give authoritative rulings on disputed questions of law and fact in accordance with legislation and case law.⁶² In a narrow sense, “judicial power” can

55 *Independent Fisheries Ltd v Minister for Canterbury Earthquake Recovery [Leave to Appeal]* [2013] NZSC 35, 2 NZLR 397.

56 At [7].

57 *Omaha Beach Residents’ Society Inc v Townsend Brooker Ltd* [2010] NZCA 413, [2011] NZRMA 1 at [33] and [46]–[50].

58 Search and Surveillance Act 2012, ss 67 and 69(2).

59 See also *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [41] (cited with approval by the Supreme Court in *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [99]).

60 *R v Gordon-Smith (on appeal from R v King)* [2008] NZSC 56, [2009] 1 NZLR 721 at [20] and [24]. See also *Hutchinson v A* [2015] NZCA 214, [2015] NZAR 1273 at [13].

61 *R v Secretary of State for the Home Department, ex p Salem* [1999] 1 AC 450 (HL) at 456–457 (cited with approval in *R v Gordon-Smith (on appeal from R v King)* [2008] NZSC 56, [2009] 1 NZLR 721 at [15]–[16]).

62 Philip Joseph *Constitutional and Administrative Law in New Zealand* (4th ed, Brookers Ltd, Wellington, 2014) at [8.2.3].

be defined as determining the rights and obligations between parties.⁶³ However, the judicial role can also include:⁶⁴

... administrative duties which need not be performed in court, but in respect of which it is necessary to bring to bear a judicial mind—that is, a mind to determine what is fair and just in respect of the matters under consideration.

- 6.59 The power to issue search warrants is an example of an administrative duty that must be performed in a judicial manner. The Court of Appeal held in *Simpson v Attorney-General [Baigent's Case]* that the issuing of a search warrant was either a “responsibility of a judicial nature” or a “judicial process” so as to fall within the scope of the immunity in section 6(5) of the Crown Proceedings Act 1950.⁶⁵
- 6.60 Judicial pre-authorisation—in the form of search warrants—emerged as a method of preventing unjustified State intrusion before it takes place.⁶⁶ The judicial officer acts as “a neutral third party, capable of acting as a true intermediary between the rights of the individual and the interests of the state”.⁶⁷
- 6.61 We think the purpose of declaratory orders under the Search and Surveillance Act, and the role of a judge in issuing them, can be described in the same way. While the issuing of declaratory orders may not be a judicial power in the narrow sense of determining the rights and obligations between parties, it does require the application of a judicial mind. In our view, the question whether a particular State intrusion is justified should be considered by an independent and impartial person wherever possible, rather than by enforcement officers. That is consistent with the rationale underlying warrants, and it is a role that has long been performed by judicial officers.
- 6.62 We reiterate that the declaratory order regime does not envisage judges providing guidance of a general nature on how enforcement activities should be carried out. In our view, that is the correct approach. Judges have expertise in applying the law to a particular set of facts. It is not their role to comment on the appropriateness of the executive using a particular type of investigatory technique in a general sense.

Grounds for issuing declaratory orders

- 6.63 The grounds for issuing declaratory orders are broader than for issuing warrants. The judge does not need to be satisfied there are reasonable grounds to believe that an offence will be committed or to suspect that evidential material will be obtained.⁶⁸ The focus is instead on whether the proposed activity is reasonable and lawful. As a consequence, declaratory orders could be sought in relation to activities that are not focused on evidence-gathering (for example, activities for the purpose of crime prevention and detection or protecting public safety).
- 6.64 Although the reason for having different grounds for issuing declaratory orders and warrants is not evident from the legislative history, it likely reflects the fact that declaratory orders are not

63 See *Love v Attorney-General for the State of New South Wales* (1990) 169 CLR 307 (HCA) at 321 (distinguished in *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA)).

64 *Royal Aquarium and Summer and Winter Garden Society Ltd v Parkinson* [1892] 1 QB 431 at 452 per Lopes LJ (cited with approval by Casey and Hardie Boys JJ in *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA) at 689 and 695).

65 *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA) at 674 (per Cooke P), 689 (per Casey J) and 695 (per Hardie Boys JJ).

66 *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [263] per Hammond J.

67 At [263].

68 See paragraphs [6.6]–[6.8].

required to be obtained and can only cover lawful activity.⁶⁹ Because of these two features, at a practical level imposing a “reasonable grounds” criterion would likely be counterproductive. It would not prevent potentially invasive activity from occurring; it would simply discourage the use of declaratory orders and thereby remove the safeguard of prior judicial consideration.

- 6.65 Trespassory searches and surveillance, and the interception of private communications, are unlawful if they are not authorised.⁷⁰ This means there is a strong incentive (and in the case of surveillance, a statutory requirement) to seek authorisation. If no warrant is obtained, the enforcement officers involved will be open to prosecution; the Crown may be liable for damages; and the admissibility of any evidence gathered as a consequence will fall to be considered under the balancing exercise in section 30 of the Evidence Act 2006.
- 6.66 By contrast, because declaratory orders deal with lawful activity, the consequences of not obtaining one are less severe. While immunity is available to enforcement officers acting under a declaratory order, if the activity carried out is lawful, there will be no need to rely on that immunity. In terms of admissibility of evidence, only if the conduct is later found to be unreasonable will the section 30 balancing exercise be undertaken – and even then, the evidence may still be admitted. Therefore, if enforcement officers were unable to meet the threshold for a declaratory order, they would likely proceed without any prior judicial authorisation.
- 6.67 In our view, the broader grounds for issuing declaratory orders are necessary to give effect to the principles of the Act that we have identified. Enforcement officers should be encouraged to seek declaratory orders wherever an activity is likely to intrude on reasonable expectations of privacy and it is not covered by a specific warrant, provision or policy statement. Restricting the availability of the orders to the evidence-gathering stage of an investigation would prevent this from occurring in relation to activities for the purpose of crime prevention and detection or public safety – even though these activities still have the potential to amount to an unreasonable search in terms of section 21 of NZBORA.
- 6.68 We think the current criteria for issuing declaratory orders can properly be applied by judges. Judges are routinely asked to assess (after the fact) whether conduct was lawful or reasonable. Provided the application sets out in sufficient detail what is proposed, making a similar assessment in advance of the activity being carried out should not cause difficulty. Indeed, the reasonableness of a proposed search is already considered in the context of warrant applications. The Act does not assume that a search is justified in the circumstances purely because the required threshold is met. The issuing officer has discretion whether to issue the warrant.⁷¹ A warrant should not be issued if the proposed conduct would be unreasonable⁷² (for example, because the proposed search would be highly intrusive and the offence under

69 We note that the residual warrant regime in the introduction version of the Search and Surveillance Bill—which would have been mandatory and able to authorise unlawful activity—included the same “reasonable grounds” threshold as search warrants: Search and Surveillance Bill 2009 (45–1), cl 59.

70 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [155] and *Choudry v Attorney-General* [1999] 2 NZLR 582 (CA) at 592–593 (trespass); Crimes Act 1961, s 216B (interception).

71 Sections 6 (search warrants) and 53 (surveillance device warrants) both provide that an issuing officer or judge *may* issue a warrant if satisfied the relevant conditions are met.

72 That would be inconsistent with s 21 of the New Zealand Bill of Rights Act 1990. The Search and Surveillance Act does not purport to override the New Zealand Bill of Rights Act; in fact, s 5 of the Act states that one of its purposes is to provide rules that “recognise the importance of the rights and entitlements affirmed in other enactments, including the New Zealand Bill of Rights Act 1990”. Furthermore, under s 6 of the New Zealand Bill of Rights Act, “[w]herever an enactment can be given a meaning that is consistent with the rights and freedoms contained in this Bill of Rights, that meaning shall be preferred to any other meaning”.

investigation is not very serious⁷³). We envisage that the assessment undertaken in relation to declaratory order applications would be similar.

- 6.69 In addition, the principles we have recommended including in the Act will provide further guidance to assist issuing officers in assessing whether it is appropriate to issue a warrant or order in the particular circumstances.⁷⁴

CLARIFYING THE DECLARATORY ORDER REGIME

- 6.70 Two submitters suggested amendments to the declaratory order provisions. Both thought it could be clearer that declaratory orders are directed to the use of a technology or method in specific circumstances rather than in a general sense. One submitter also suggested clarifying that the orders cannot authorise unlawful or unreasonable activity; and permitting a judge to attach conditions to an order.
- 6.71 As we have discussed above, we think the Act is already clear that declaratory orders must relate to specific circumstances.⁷⁵ We do not therefore recommend any amendments in this respect. However, we do think some other amendments are appropriate to clarify the effect of declaratory orders.
- 6.72 As we foreshadowed in the preceding discussion, the key difference between declaratory orders and warrants is that declaratory orders cannot authorise activity that is unlawful. In other respects, we think declaratory orders should be viewed as another type of warrant. Like a warrant, they provide judicial authorisation for a proposed activity to be carried out in a specified context, and confer immunity for acts done in reliance on the order. In our view, much of the confusion surrounding declaratory orders could be remedied by making the relevant provisions more consistent with the warrant provisions in the Act.

Renaming “declaratory orders”

- 6.73 The name “declaratory orders” suggests the orders are akin to orders under the Declaratory Judgments Act 1908. We think that removing the term “declaratory” may help to clarify the position. However, while we think declaratory orders are similar to warrants in many respects, it is important to reflect the fact that the orders only relate to lawful activity. Calling them a “warrant” might imply they are broader in scope, since warrants traditionally authorise unlawful activity.
- 6.74 We recommend renaming declaratory orders as “orders authorising specific activity”, or something similar.⁷⁶ In our view, this would more accurately reflect the nature of the orders.

Repealing subsection 65(2) and stating when declaratory orders are invalid

- 6.75 Subsection 65(2) states that “[a] declaratory order is advisory in character and does not affect the jurisdiction of any court to determine whether the activity that was the subject of the order was reasonable and lawful.” We have been unable to discern from the materials relating to the Search and Surveillance Bill why subsection 65(2) was inserted. It seems likely that the reference to the orders not affecting the jurisdiction of a court was intended to address the

73 The extent of the intrusion on privacy and the reason for the search are relevant in assessing reasonableness under s 21 of the New Zealand Bill of Rights Act 1990: *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [172] (per Blanchard J, McGrath and Gault JJ concurring) and [223] (per Tipping J). We discuss this in Chapter 4 at paragraphs [4.52]–[4.55].

74 See Chapters 3 and 4.

75 See paragraphs [6.6] and [6.9].

76 For example, the title of s 68 might be rephrased as “judge may make order authorising specific activity”. In practice the orders would likely be referred to by a shortened name, such as a “section 68 order” or “specific activity order”.

concern raised by opposition Members of Parliament that a later court may feel unable to depart from the orders.⁷⁷ The reason for the reference to orders being “advisory in character” is less clear. It may have been an attempt to emphasise that the orders cannot authorise unlawful activity.

- 6.76 The statement in subsection 65(2) that the orders are “advisory” in character suggests they amount to “advisory opinions”, which the courts have traditionally been reluctant to give. As we have discussed, we do not consider that to be the case. Declaratory orders must relate to specific fact situations in the same way as warrants.
- 6.77 Declaratory orders and warrants are also the same in the sense that a later court can find that the conduct was unlawful or unreasonable (although enforcement officers are immune from liability if they act in good faith).⁷⁸ Despite this, the Act does not state that a warrant does not bind a later court. Instead, it provides that warrants (and production orders) are invalid where the relevant preconditions for issuing them are not met.⁷⁹ The fact that declaratory orders are framed in a different way may suggest they have a different effect, which we do not consider is—or should be—the case.
- 6.78 For those reasons, we recommend that subsection 65(2) should be repealed. In its place, the Act should state that a declaratory order is invalid if the activity it covers is unlawful or unreasonable. As well as providing greater consistency with other warrants and orders under the Act, this should make it clear beyond doubt that declaratory orders cannot authorise activity that is unlawful or unreasonable. While this is currently implied by sections 65 and 68, it is not expressly stated.
- 6.79 The immunity in section 165(b) should continue to protect anyone who does an act in good faith that is covered by a declaratory order even if the order is later found to be invalid.⁸⁰ This will ensure that enforcement officers and any person assisting them can rely on the orders and will not be penalised if a judge makes an error in issuing one (for example, if the order purports to authorise an act that is unlawful).

Expressly enabling judges to impose conditions

- 6.80 The search warrant and surveillance device warrant provisions in the Act specifically enable an issuing officer to impose conditions when issuing the warrant or order.⁸¹ The declaratory order provisions do not. One submitter suggested that should be rectified.
- 6.81 Given that the issuing of a declaratory order is discretionary, we think it would already be open to a judge to place constraints on how the proposed activity will be carried out to ensure it is reasonable. That was clearly envisaged in the departmental report on the Search and Surveillance Bill.⁸² However, for the avoidance of doubt, we agree that section 69 be amended to clarify that conditions may be imposed.

⁷⁷ See paragraph [6.18].

⁷⁸ See paragraphs [6.31] and [6.45]–[6.46].

⁷⁹ Search and Surveillance Act 2012, s 107 (search warrants). This section also applies to surveillance device warrants (s 58) and production orders (s 77).

⁸⁰ We note that, under s 27 of the Crimes Act 1961, a person who is authorised to execute a warrant or “process” issued by a court (or any person assisting them) is justified in doing so even if the court had no jurisdiction to issue the warrant or process. It is likely that this section would apply to a declaratory order or production order issued under the Search and Surveillance Act (as a “process” issued by the court). However, for the sake of clarity there may be value in expressly stating in the Act that the immunities in s 165 continue to apply if the relevant warrant or order is found to be invalid.

⁸¹ Search and Surveillance Act 2012, ss 55(2) and 103(3)(b).

⁸² Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [314]: “The declaratory order may contain detail as to the conditions under which use of the new device, technique, or procedure would be reasonable (eg, use of heat sensing technology is reasonable and lawful only if not directed at bathrooms)”.

Aligning procedural requirements with warrants

6.82 Finally, we note there are a number of provisions that apply to search warrants and surveillance device warrants but not to declaratory orders. Given that we see declaratory orders as being similar in effect to warrants, we think they should be subject to the same requirements and procedures unless there is good reason to take a different approach. We therefore recommend that the following provisions should apply to declaratory orders, as they do for warrants:⁸³

- section 98(2) (which allows the issuing officer to require further information from the applicant);
- section 99 (which requires an application to be supported by a statement by the applicant confirming its truth and accuracy);
- section 100 (which sets out the available methods for making applications, including provision for oral and electronic applications);
- section 101 (which requires the applicant and the Registrar of the relevant District Court to retain records of warrant applications and other documentation); and
- section 105 (which allows for electronic or fax transmission of warrants).

RECOMMENDATION

R13 The following amendments should be made to clarify the provisions in the Act that deal with declaratory orders:

- (a) The name “declaratory orders” should be changed to “orders authorising specific activity” or something similar.
- (b) Subsection 65(2) (which states that a declaratory order is advisory in character) should be repealed.
- (c) A new provision should be inserted stating that a declaratory order is invalid if the activity it covers is unlawful or unreasonable.
- (d) The Act should be amended to ensure that section 165(b) (which states that every person is immune from civil or criminal liability for any act done in good faith that is covered by a declaratory order) applies even if the order is later found to be invalid.
- (e) Section 69 should be amended to state that the judge can impose conditions on a declaratory order.
- (f) Sections 98(2) (relating to requirements for further information), 99 (application must be verified), 100 (mode of application for a search warrant), 101 (retention of documents) and 105 (transmission of search warrant) should apply to declaratory orders, with any necessary modifications.

⁸³ We note these provisions are applied to surveillance device warrants by ss 52(2) and 58.



Part 2 **SURVEILLANCE**

Chapter 7

Scope of surveillance powers

INTRODUCTION

- 7.1 In this chapter, we discuss the surveillance regime in the Search and Surveillance Act 2012 (the Act). We identify, and make recommendations to address, a number of areas where the regime has not kept pace with developments in technology. We also address a number of more discrete issues with the operation of the regime that have become apparent since its enactment.
- 7.2 In our Issues Paper we raised a number of questions about the kind of activity that should be regulated by the surveillance regime. We discuss some of those questions in other parts of this Report.¹ In this chapter:
- We outline the current scope of the surveillance regime.
 - We identify a number of new surveillance technologies that the regime does not adequately cover. Specifically, we discuss surveillance using technology such as computer programs rather than “devices”, extrasensory technology (such as thermal imaging and x-ray), and data surveillance (such as monitoring the keys struck on a computer keyboard or using cell-site simulators). We propose amendments to require a warrant for these types of surveillance.
 - We explain that the regime does not always allow surveillance powers to be exercised in emergency situations, or to locate high-risk offenders who tamper with electronic monitoring devices. We recommend amendments to address this.
- 7.3 First, there is a matter of terminology that we need to clarify. The Act currently refers to “surveillance device warrants”. As we will explain, these warrants are only required where surveillance involves the use of certain devices. Later in this chapter, we recommend that the regime be expanded to capture electronic surveillance that does not involve the use of a “device”. Therefore, except where we are specifically discussing the existing surveillance device warrant regime, we refer throughout this Report to “surveillance warrants”.

OVERVIEW OF THE SURVEILLANCE DEVICE REGIME

- 7.4 The Act does not define “surveillance”.² Instead, it refers to the use of “surveillance devices”. “Surveillance device” is defined as an interception device, tracking device or visual surveillance device.³ Unless an exception applies,⁴ enforcement officers⁵ must obtain a surveillance device warrant in order to use:⁶

1 See Chapters 9 (interception and tracking), 11 (public surveillance) and 15 (covert operations).

2 In our Issues Paper we suggested that “surveillance” could be understood as the observation or monitoring of people, places, things, data or communications: Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [2.20] [Issues Paper].

3 Search and Surveillance Act 2012, s 3 (definition of “surveillance device”).

4 See paragraph [7.8].

5 Enforcement officers are constables and any person authorised to exercise powers listed in the Schedule or to which Part 4 of the Act applies (s 3, definition of “enforcement officer”). This includes people with regulatory powers of entry, search, inspection, examination, or seizure.

6 Search and Surveillance Act 2012, s 46.

- an interception device to intercept a private communication;
 - a tracking device (unless no trespass is involved and the purpose is solely to detect whether a thing has been opened, tampered with or otherwise dealt with);
 - a surveillance device in a manner involving trespass to land or goods; or
 - a visual surveillance device to:
 - observe and/or record private activity in private premises; or
 - observe and/or record private activity in the curtilage⁷ 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).
- 7.5 Enforcement officers are not required to obtain warrants to carry out surveillance using other types of devices, or surveillance not using a device.⁸ However, the Act also does not allow warrants to be issued in such cases. This means surveillance using other types of devices or not using a device is unlikely to be used at all if it would breach the law or amount to an unreasonable search in terms of section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA).
- 7.6 Surveillance device warrants can only be issued by judges⁹ (in comparison to search warrants, which can be issued by any issuing officer¹⁰). A judge may issue a surveillance device warrant if they are 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.¹¹ Relevant offences are those in respect of which the enforcement officer is authorised to apply for a warrant to enter premises under the Act or any other enactment listed in the Schedule to the Act.¹²
- 7.7 Two additional restrictions apply if the warrant would permit either visual trespass surveillance (that is, visual surveillance involving trespass to land or goods)¹³ or the use of an interception device:¹⁴
- The warrant must relate to an offence that is punishable by at least seven years' imprisonment or certain other specified offences.¹⁵
 - The warrant can only be applied for by a constable or an enforcement officer employed by an approved law enforcement agency.¹⁶ Section 50 allows the Department of Internal Affairs (DIA) or New Zealand Customs Service to be approved by Order in Council for this purpose. However, this has not yet occurred, so at present only constables can apply for these warrants.

7 "Curtilage" is not defined in the Act. It includes the land immediately surrounding a house or building (such as a garden, yard or field) and any closely associated buildings and structures: see *Butterworths New Zealand Law Dictionary* (7th ed, LexisNexis, Wellington, 2011).

8 Warrants are only required in the situations set out in s 46 (see paragraph [7.4]) and can only be issued in relation to the use of a "surveillance device" (see ss 51(a)(ii) and 55(3)(c)).

9 Section 53.

10 Section 6. An "issuing officer" is defined in s 3 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.

11 Section 51.

12 Section 51(a)(i). The term "relevant offence" is not used in the Act, we simply use it here for convenience.

13 Section 3 (definition of "trespass surveillance").

14 We discuss these restrictions in more detail in Chapter 8.

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

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

- 7.8 The Act recognises some exceptions to the requirement to obtain a surveillance device warrant. An enforcement officer does not require such a warrant to:¹⁷
- record what they observe 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.
- 7.9 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.¹⁸ An enforcement officer who carries out warrantless surveillance must report to a judge within one month.¹⁹ The judge may make directions about the retention or destruction of the material obtained, report unauthorised surveillance to the chief executive of the enforcement agency or order that the subject of the surveillance be notified.²⁰

SURVEILLANCE NOT COVERED BY THE REGIME

- 7.10 As we have discussed, the surveillance device warrant regime in the Act only requires a warrant to be obtained—and only permits one to be issued—in relation to surveillance using interception, tracking and visual surveillance devices.²¹ This leaves two categories of surveillance that the regime does not address at all: surveillance not using a “device” and surveillance using devices that do not fall within one of the existing three categories.²²
- 7.11 “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”.²³ This implies that “device” is intended to carry its ordinary meaning of a tangible thing, rather than an intangible thing such as a computer program.
- 7.12 The rationale for restricting the regime to the use of certain “devices” is not discussed in the Law Commission’s 2007 Report, *Search and Surveillance Powers*. That approach appears simply to have been carried over from the limited interception device and tracking device warrant provisions that already existed in the Crimes Act 1961 and the Summary Proceedings Act 1957.²⁴ However, the Law Commission acknowledged this limitation and anticipated that the residual warrant regime it recommended would cover surveillance not using “devices” or using other types of devices.²⁵
- 7.13 As we discussed in Chapter 6, residual warrants were then changed during the passage of the Bill to “declaratory orders”, which cannot authorise unlawful activity. This meant that there was no remaining avenue for obtaining a warrant for other types of surveillance.

17 Section 47(1).

18 Section 48.

19 Section 60.

20 Section 62.

21 See paragraphs [7.4]–[7.5].

22 Surveillance in public places, or relating to publicly available information, is also not generally covered by the regime. This is discussed in Chapter 11.

23 Search and Surveillance Act 2012, s 3.

24 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.67].

25 At [11.121].

Issues Paper

- 7.14 In our Issues Paper, we explained that electronic surveillance can increasingly be carried out using technology—such as computer programs—that is not a “device” as that word is traditionally understood.²⁶ For example, software can monitor the websites a person visits or intercept their emails. Currently, the Act does not provide for the use of these types of technology, even though they may have the same effect as the use of a surveillance device. Enforcement officers are not required to seek a warrant to use surveillance technology that is not a “device”, but equally the Act does not provide for warrants to be issued in such cases.
- 7.15 We also identified two classes of “devices” that could be used for surveillance purposes but are not covered by the Act:²⁷
- Devices such as thermal imaging devices (often called FLIR – Forward Looking Infrared) or chemical residue detectors, which allow the user to detect heat emanating from a building and chemical residue (such as drug residue) inside luggage.²⁸ In this Report, we refer to this class of devices as “extrasensory”, as they enable the user to observe or detect things that cannot be perceived using natural senses. X-ray is another example of technology falling within this category.
 - Data surveillance devices, which record or monitor the input of information into, or the output of information from, a computer or other electronic device. This would include, for example, devices that log key strokes on a computer. The same functions can be performed by software (as opposed to hardware).
- 7.16 We noted that the installation or use of these technologies and devices may involve unlawful activity (such as trespass to install a data surveillance device or software on a computer or unauthorised access to a computer system).²⁹ The fact that the Act does not provide an authorisation framework for these technologies is therefore a barrier to their use. Our Issues Paper suggested that this may be undesirable, given that these technologies often perform the same function as devices that can currently be authorised (such as the use of software rather than a device to intercept communications) or in some cases may be less intrusive than activities that are already permitted (such as the use of FLIR to detect heat emanating from a building rather than physically entering and searching it).³⁰
- 7.17 We asked for submitters’ views on whether the surveillance regime in the Act should be broadened to cover a wider range of electronic surveillance, including the use of technology such as computer programs.³¹

Submissions

- 7.18 All of the submitters who addressed this issue supported amending the Act to regulate a wider range of electronic surveillance. They differed on how that should occur. The New Zealand Law Society argued that each surveillance technique that is permitted should be specifically listed in the Act rather than broadening the language of the warrant provisions. This would ensure that Parliament expressly considers whether there is sufficient justification for the use of each.

26 Issues Paper, above n 2, at [3.67].

27 At [3.62]–[3.65].

28 At [3.61].

29 At [3.70]–[3.71].

30 At [3.67] and [3.72].

31 At [3.74]–[3.76] and question 8.

- 7.19 Other submitters thought the language of the surveillance device warrant provisions should be wider or that the use of new surveillance technologies should be dealt with through a residual warrant regime. The Department of Internal Affairs (DIA) suggested that the concept of a “device” could be removed to enable a warrant to be obtained for any “surveillance”, similar to a residual warrant. The New Zealand Criminal Bar Association also supported a “catch-all” for new and developing forms of electronic surveillance.
- 7.20 An alternative submission by DIA was that, rather than removing the concept of a “device”, the term “surveillance device” could be broadened to include things such as the use of computer programs. New Zealand Police also supported amendments to capture both electronic surveillance not using a device and the use of data surveillance devices.

Surveillance not using “devices”

- 7.21 For reasons we have already discussed in Chapter 6, we do not recommend the introduction of a residual warrant regime. For the same reasons, we consider it would be inappropriate to enable a judge to grant authorisation for any “surveillance”. While “surveillance” is not defined in the Act, its ordinary meaning captures any ongoing observation or monitoring of people, places, things, activity or data, regardless of the method used.³² This would substantially broaden the surveillance regime in the Act, giving judges the power to authorise the use of any new technologies or methods. Where new types of surveillance are substantively different to the types of surveillance already recognised in the Act, we think it is appropriate that they should be considered by Parliament.³³
- 7.22 However, we consider that there is scope to make the current provisions somewhat more flexible without infringing on that principle. Given that Parliament has decided that interception, visual surveillance and tracking should be possible in appropriate cases, we see no reason to distinguish based on whether the technology used is a physical device or is intangible. Regardless of the means used, the level of intrusion involved and the result of the surveillance are likely to be the same. If anything, the use of intangible technology (such as software) may be less intrusive than the use of a device in some cases, if it permits the interception, visual surveillance or tracking to occur without an enforcement officer needing to enter private premises or interfere with personal property to install a device.
- 7.23 There is precedent in overseas legislation for surveillance warrant provisions covering more than just “devices”. As we explained in our Issues Paper, some of the warrant provisions in Australian and Canadian legislation specifically refer to computer programs.³⁴ The relevant United Kingdom legislation is generally not limited to the use of devices or technology – it focuses on the outcome rather than the means by which it is achieved.³⁵
- 7.24 We considered whether the reference to “devices” in the Act should be removed altogether. The Act could require a warrant to carry out interception, tracking or visual surveillance. However, we could see problems with that approach. It would capture things that an enforcement

32 Definitions include “close observation, especially of a suspected person” (Tony Deverson and Graeme Kennedy (eds) *New Zealand Oxford Dictionary* (Oxford University Press, Melbourne, 2005)); “continuous observation of a place, person, group, or ongoing activity in order to gather information” (*Dictionary.com* “Surveillance” < www.dictionary.com >); “constant observation of a place or process” (*Collins English Dictionary* “Surveillance” < www.collinsdictionary.com >); and “scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts” (George Ritzer (ed) *Encyclopedia of Social Theory* (Sage Publications, Thousand Oaks, 2005) at 871).

33 Where a new surveillance technique is lawful, the enforcement agency could seek a declaratory order (see Chapter 6) or a new policy statement could be issued (see Chapter 5).

34 Issues Paper, above n 2, at [3.62] and [3.69]; Surveillance Devices Act 2004 (Cth), s 6 (definition of “data surveillance device”); Criminal Code RSC 1985 c C-46, ss 492.1(8) (definition of “tracking device”) and 492.2(6) (definition of “transmission data recorder”).

35 See, for example, Investigatory Powers Act 2016 (UK), ss 4, 15(2) and 99(2) and (4); Regulation of Investigatory Powers Act 2000 (UK), s 26(3).

officer hears or observes with their ordinary senses. For example, inadvertently overhearing a conversation could amount to “interception” and watching a person walk into a building might be “tracking”. While specific exceptions could be included to address these examples, we were concerned that such a broad reframing of the warrant regime might have unintended consequences.

- 7.25 Instead, we propose that section 46 (which sets out when a surveillance device warrant is required) should be amended so that a warrant must be obtained to use interception, tracking or visual surveillance “technology” in the circumstances specified in the Act.³⁶ “Technology” is a broad term that is capable of capturing both physical and intangible things.³⁷ The current definitions of “interception device”, “tracking device” and “visual surveillance device” in section 3 should be replaced with definitions of “interception technology”, “tracking technology” and “visual surveillance technology”. These definitions should be drafted in a way that includes the use of computer programs, devices and other technological aids. In other respects, the definitions would mirror the current ones (except to the extent that specific amendments are proposed elsewhere in this Report).³⁸ Surveillance device warrants should be renamed “surveillance warrants” to reflect these changes.
- 7.26 We note that this will create an inconsistency with the Crimes Act 1961, which only prohibits the interception of private communications “by means of an interception device”.³⁹ This should not cause any practical difficulty, as enforcement officers will still be able to obtain authorisation for any activity that would otherwise fall within the interception offence provision. It will mean that a warrant is required in circumstances that would not amount to an offence; however, that is already the case in relation to tracking and visual surveillance (which do not have corresponding offence provisions). We have not considered whether the Crimes Act provision should be amended as that is outside the scope of this review. However, there may be merit in the Government looking at this issue in the context of any future review of the relevant provisions in the Crimes Act.

Extrasensory observation

- 7.27 In our meetings with experts and officials, it was suggested to us that the use of some extrasensory technologies, such as FLIR and x-ray, may already fall within the definition of “visual surveillance”. Experts and officials considered this an appropriate way to deal with these kinds of technologies, although they acknowledged it could be made clearer that they are covered by the definition.
- 7.28 “Visual surveillance device” is defined in section 3 of the Act as follows:

visual surveillance device—

- (a) means any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to observe, or to observe and record, a private activity; but
- (b) does not include spectacles, contact lenses, or a similar device used to correct subnormal vision of the user to no better than normal vision

³⁶ See paragraph [7.4] and s 46 of the Search and Surveillance Act 2012.

³⁷ Dictionary definitions include: “the study or use of the mechanical arts and applied sciences” (Tony Deverson and Graeme Kennedy (eds) *New Zealand Oxford Dictionary* (Oxford University Press, Melbourne, 2005)); “[t]he application of scientific knowledge for practical purposes, especially in industry” (*Oxford English Dictionary* “Technology” < <https://en.oxforddictionaries.com/> >); and “[t]he practical application of knowledge especially in a particular area” (*Merriam-Webster* “Technology” < www.merriam-webster.com >).

³⁸ Chapter 9 at paragraphs [9.69]–[9.74].

³⁹ Crimes Act 1961, s 216B.

- 7.29 “Private activity” is activity that any one or more of the participants ought reasonably to expect is observed or recorded by no one except the participants.⁴⁰
- 7.30 We agree that some extrasensory technology is “capable of being used to observe, or to observe and record, private activity”. While some definitions of “observe” refer only to “watching” a person or thing, most are wider and include noticing, perceiving or detecting something.⁴¹ However, the use of the term “visual surveillance” may be taken to imply that the observation is of something that may be “seen” in the ordinary sense, as opposed to things such as heat that are not visible without the use of technology. The position therefore lacks certainty.
- 7.31 A warrant is only required to use a visual surveillance device if it involves observing private activity in private premises, or private activity in the curtilage of private premises if the observation exceeds three hours.⁴² In our view, this is a sensible approach for extrasensory observation. As with other visual surveillance, requiring a warrant to use extrasensory technology in public places could cause practical difficulties. For example, we understand that the Police Eagle helicopter uses FLIR to track fleeing offenders from the air. In the course of doing so it will necessarily observe the curtilage of private property as well – although only in a fleeting manner. Applying the visual surveillance provisions, a warrant would not be required in these circumstances. We think that is appropriate given the relatively low level of privacy intrusion involved.
- 7.32 We therefore recommend that the definition of “visual surveillance device” (which, if recommendation 14 is adopted, will become “visual surveillance technology”) be amended to clarify that it includes any device or program that can be used to observe private activity by extrasensory means (for example, thermal imaging and x-ray technology).⁴³ Where extrasensory technology is used in public places, different considerations arise. We discuss this in Chapter 11.

Extrasensory observation as “trespass” surveillance

- 7.33 As we have discussed above,⁴⁴ warrants permitting visual trespass surveillance can currently only be issued to constables and in relation to serious offences, in recognition of the high level of privacy intrusion involved.
- 7.34 In terms of intrusiveness, extrasensory technology raises different concerns. A video camera will generally only be able to observe private activity inside private premises if it is installed inside the premises, which will involve trespass. By contrast, sophisticated extrasensory technology may be capable of effectively “seeing” inside private premises without any trespass occurring. Handheld “through-the-wall sensors” are already available commercially, although they currently only work at short range.⁴⁵ These sensors use electromagnetic waves to detect the presence of people and objects inside a building and whether they are moving. “Backscatter” x-ray is also now strong enough to produce detailed images of the contents of closed vehicles

40 Search and Surveillance Act 2012, s 3.

41 Tony Deverson and Graeme Kennedy (eds) *New Zealand Oxford Dictionary* (Oxford University Press, Melbourne, 2005): “observe” is defined as “perceive, note; take notice of; become conscious of”.

42 Section 46. The three-hour time limit for warrantless observation of curtilage is over a 24-hour period. A warrant is also required if the observation exceeds eight hours in total. In calculating these time periods, observation is counted if it is for the purposes of a single investigation or connected series of investigations.

43 “Extrasensory” is defined as “regarded as derived by means other than by the known senses” (Tony Deverson and Graeme Kennedy (eds) *New Zealand Oxford Dictionary* (Oxford University Press, Melbourne, 2005)) or “occurring or seeming to occur apart from, or in addition to, the normal function of the usual senses” (*Webster’s New World College Dictionary* “Extrasensory” (4th ed, Houghton Mifflin Harcourt, 2010)).

44 See paragraph [7.7]. See also Chapter 8 at paragraphs [8.10]–[8.15] and [8.47]–[8.52].

45 Lars Ericson and others “Through-the-Wall Sensors for Law Enforcement: Best Practices” (United States Department of Justice, National Institute of Justice, 2014).

and cargo containers.⁴⁶ It seems entirely possible that technology will soon make it realistic for enforcement agencies to monitor activity inside private premises from a vehicle parked on the street outside.

- 7.35 In our view, the stricter requirements that currently apply to visual trespass surveillance should apply whenever visual surveillance technology is used to observe private activity in private premises (but not on the curtilage of private premises). Although physical trespass may not be involved, the intrusion on privacy in such cases would be similar.
- 7.36 We would not expect these stricter requirements to apply in cases where visual surveillance of a public area or of the curtilage of private property inadvertently sees into an uncovered window. That is because the definition of “private activity” is unlikely to cover activity occurring behind an uncovered window that can be seen from a public place by any passer-by. The position might be different if, for example, the surveillance uses the zoom function on a camera to see detail that could not be discerned with the naked eye.

Data surveillance technology

- 7.37 Australian surveillance device legislation requires authorisation to use a “data surveillance device”. This 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”.⁴⁷ “Computer” is defined as “any electronic device for storing or processing information”.⁴⁸
- 7.38 Some surveillance methods that would fall within the definition of “data surveillance device” in the Australian legislation would already be covered by one of the other categories of surveillance already regulated by the Search and Surveillance Act. For example, a program that forces a computer to broadcast its Internet Protocol (IP) address so that it can be located would be captured by the definition of “tracking device”; and obtaining emails while they are in the course of transmission would use an “interception device”.
- 7.39 However, there are other types of data surveillance that may not be covered by the existing warrant provisions in the Act, depending on the specific technology used.⁴⁹ Examples include:
- the use of computer programs or devices to monitor and/or record:
 - the keystrokes that a user types on the keyboard of a computer or other electronic device (“keystroke logging”);⁵⁰
 - the web browsing history of a user or electronic device (“browser history monitoring”); and
 - the use of International Mobile Subscriber Identity (IMSI) catchers or cell-site simulators, which force mobile electronic devices to transmit data to them by mimicking cell towers.⁵¹

We briefly outline below how these technologies can be used and the level of privacy intrusion that may be involved. We conclude that the surveillance regime should be extended to cover these types of technology by expressly requiring a warrant for their use.

46 Joseph Callerame *X-Ray Backscatter Imaging: Photograph Through Barriers* (International Centre for Diffraction Data, 2006).

47 Surveillance Devices Act 2004 (Cth), s 6 (definition of “surveillance device”).

48 Surveillance Devices Act 2004 (Cth), s 6 (definition of “computer”).

49 Some of these methods might qualify as another form of surveillance in some cases. For example, keystroke logging could be achieved by setting up a video camera to watch the keys struck but may also occur without any visual observation by installing a physical device or software into the target computer.

50 Keystroke logging would likely be captured by the Australian definition of “data surveillance device”: Australian Law Reform Commission *Serious Invasions of Privacy in the Digital Era* (ALRC DP80, 2014) at [13.26].

51 An International Mobile Subscriber Identity (IMSI) is a number located in a mobile phone’s subscriber identification module (SIM) card, which identifies the subscriber.

Keystroke logging and browser history monitoring

- 7.40 Keystroke logging and browser history monitoring have the potential to be valuable law enforcement tools, particularly as encryption makes it easier for offenders to cover their tracks. For example, people who deal in objectionable material (such as child exploitation material) may store it in an encrypted form that is password protected, so a search of their electronic devices may not reveal any evidential material. While the Act requires a person to provide access information such as passwords on request by a person exercising a search power, there is little incentive to comply with that requirement where the penalty for the offence being investigated is high.⁵² We discuss that issue in Chapter 12. It may also be unclear from a search of the person's devices what facilities (such as websites or "dark web" forums) are being used to trade the objectionable material. Keystroke logging and/or browser history monitoring technology may allow an enforcement agency to identify where the material is being stored or traded and to obtain the information required to access that facility.
- 7.41 The use of such technology can, however, be intrusive. It can provide a full picture of everything a person does using a particular device. By monitoring a person's browsing history, an enforcement agency might be able to tell what health ailments they are suffering from; what their sexual preferences, religious beliefs and political affiliations are; or whether they are having an extra-marital affair. If a person's keystrokes are monitored, the content of their private emails or other electronic messages may also be disclosed. There is also a risk that the privacy of people other than a suspect will be infringed. For example, in a family situation, multiple people may use the same electronic device.

IMSI catchers

- 7.42 IMSI catchers, also known as cell-site simulators, are devices that mimic cell towers. They force electronic devices with SIM cards in the surrounding area to transmit: their location; data that can be used to identify their users; and information about the numbers the device has called or sent messages to.⁵³ Depending on the configuration of the IMSI catcher, the network connectivity of the electronic devices may be disrupted while this occurs because the data received by the IMSI catcher is not redirected to the real cell tower.⁵⁴ Some models of IMSI catchers are also capable of collecting the content of calls or messages.⁵⁵
- 7.43 IMSI catchers can be used to locate a known device – for example, an enforcement agency may be able to track down a fugitive who is believed to be within a particular area by locating their cell phone.⁵⁶ In these cases, data will be received from other phones for a very short period of time while the IMSI catcher is finding the target phone. This kind of IMSI catcher use would likely be captured by the definition of "tracking technology".
- 7.44 However, IMSI catchers can also be used to obtain other information. For example, they could be used to discover the phone numbers a target device is communicating with at a given time

52 Section 130.

53 Committee on Oversight and Government Reform *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* (United States House of Representatives, 19 December 2016) at 10 (figure); David Anderson QC *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) at [4.73]; C Justin Brown and Kasha M Leese "Stingray Devices Usher in a New Fourth Amendment Battleground" *The Champion* (June 2015) < www.nacdl.org > at 13–14.

54 Tamir Israel and Christopher Parsons *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada* (Telecom Transparency Project and Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, August 2016) at 12.

55 Committee on Oversight and Government Reform *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* (United States House of Representatives, 19 December 2016) at 13; David Anderson QC *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) at [4.73]; C Justin Brown and Kasha M Leese "Stingray Devices Usher in a New Fourth Amendment Battleground" *The Champion* (June 2015) < www.nacdl.org > at 14.

56 Committee on Oversight and Government Reform *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* (US House of Representatives, 19 December 2016) at 12.

or to identify people who are present at a gathering of an organised criminal group.⁵⁷ These functions are unlikely to fall within the definition of “tracking technology”. The definition of “intercept” will not necessarily apply either, because it requires a communication to be acquired while it is taking place or in transit.⁵⁸ IMSI catchers—at least in some cases—are the end-point for data. The data is not redirected to the real cell tower;⁵⁹ rather, it is “received” by the IMSI catcher.

- 7.45 The ability of IMSI catchers to help identify targets and their associates has obvious potential to assist in law enforcement investigations, particularly in relation to offences committed by criminal groups (such as terrorism and drug offending). However, using IMSI catchers may also involve capturing a significant amount of data from electronic devices that is not linked to a suspect. A recent report by the United States House of Representatives on the use of cell-site simulation technology explains:⁶⁰

To use the device as an investigative tool, law enforcement deploys the device at a known location of the target and obtains every IMSI number in the vicinity at the time of deployment. By deploying the device numerous times in numerous locations where the targeted individual is present, law enforcement collects a list of IMSI numbers for each cell phone present at every location where the device was deployed. The device analyzes this list to determine if there were common IMSI numbers at each location. By a process of elimination, the common IMSI numbers are identified as likely to be those of the target’s phone, and individuals associated with the target. Law enforcement can then work with cellular service providers to determine telephone numbers and billing information associated with specific IMSI numbers.

Likewise, the devices could be deployed at groups of people who assemble at different times in different places to eventually determine the identities of individuals whose IMSI numbers become associated with that group. When used as an investigative tool, the device stores the identifying numbers for a limited period of time to analyze them for the purpose of distinguishing the targeted device(s).

- 7.46 IMSI catchers are currently used by enforcement agencies overseas, although the manner in which they are used is closely guarded.⁶¹ In the United States, a Department of Justice policy requires a search warrant to be obtained before they are used.⁶²

Requiring a warrant to use data surveillance technology

- 7.47 Where data surveillance technology does not fall within one of the categories of surveillance recognised in the Act, enforcement agencies will usually be unable to use it. Data surveillance without a warrant is likely to amount to unauthorised access to a computer system under the Crimes Act.⁶³ It may also involve trespass (for example, to install a data surveillance device or software onto a computer) or amount to an unreasonable search under section 21 of NZBORA.

57 As described in paragraph [7.45].

58 Search and Surveillance Act 2012, s 3 (definition of “intercept”). The current interception regime is also limited to the interception of “private communications”, which is unlikely to include metadata. However, we recommend below that this be changed (see paragraphs [9.10]–[9.18]).

59 We note that it appears some IMSI catchers are capable of rerouting data to the real cell tower when they are in “camping mode” (enabling them to intercept the content of communications): in such cases the interception regime might apply. However, enforcement agencies overseas primarily use IMSI catchers in “identification mode”, which does not have this feature.

60 Committee on Oversight and Government Reform *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* (United States House of Representatives, 19 December 2016) at 12.

61 See United States Department of Justice “Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators” (3 September 2015); *State of Maryland v Andrews* No 1496 Md App 1 (Md Ct Spec App 2016); “Controversial snooping technology used by at least seven police forces” *The Guardian* (online ed, London, 10 October 2016); “Vancouver police confirm use of ‘stingray’ surveillance technology” *The Guardian* (online ed, London, 10 August 2016).

62 United States Department of Justice *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* (3 September 2015).

63 Crimes Act 1961, s 252. “Access” is defined broadly in s 248 as “instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system”.

- 7.48 As we have discussed above, there are both risks and benefits associated with data surveillance technology. It has the potential to significantly assist in the investigation of offences that are otherwise difficult to detect, such as child exploitation and organised crime.⁶⁴ However, it may also allow an enforcement agency to access detailed information about a person's private life and—particularly in the case of IMSI catchers—may require the collection of data about innocent third parties. On balance, we consider that enforcement agencies should be able to use data surveillance technology, but that it should be subject to strict controls to ensure its use is sufficiently targeted and limited to serious cases.
- 7.49 We recommend the Act require enforcement officers to obtain a surveillance warrant to use “data surveillance technology”. “Data surveillance technology” should be defined as a device, program or other technological aid capable of being used to monitor or record the input of information to, or output of information from, an electronic device (with some specific exclusions, which we discuss below).⁶⁵
- 7.50 In terms of intrusiveness, we consider data surveillance to be similar to interception. Both involve obtaining significant amounts of information that may reveal private details about a person's life and may relate to people other than the suspect. It is therefore appropriate to treat data surveillance in the same way as interception under the Act. This will require amendments to sections 45, 49(5) and 50 so that the higher threshold and the restrictions on who can apply for warrants authorising interception and visual trespass surveillance also apply to data surveillance.⁶⁶
- 7.51 The requirement to obtain a surveillance warrant will mean that data surveillance technology can only be used where there are reasonable grounds to suspect that an offence has been, is being or will be committed, and to believe that the use of the technology will obtain evidential material in respect of the offence.⁶⁷ A judge considering a warrant application relating to the use of data surveillance technology will also need to have regard to the principles we have recommended including in the Act, such as proportionality and minimal intrusion.⁶⁸

Exclusions from the definition of “data surveillance technology”

- 7.52 The definition of “data surveillance technology” should exclude anything that falls within the definition of “interception technology” or “visual surveillance technology”. This will ensure that multiple warrants are not required for the same activity. The position in relation to tracking is different, because tracking is not subject to the higher threshold in section 45.⁶⁹
- 7.53 We also suggest that section 47 (which sets out some situations in which surveillance device warrants are not required) be amended to recognise two exceptions to the requirement to obtain a warrant to use data surveillance technology. First, an enforcement officer should not require a warrant to monitor or record inputs or outputs from an electronic device that they are lawfully in possession of. This would ensure that a warrant is not required for ordinary use of devices that enforcement officers are entitled to access (including a device that is being searched pursuant to a search power).

64 See paragraphs [7.40]–[7.45].

65 As we discuss in Chapter 12 at paragraph [12.5], we use the term “electronic device” broadly to describe any device that is capable of storing data. This would include, for example, computers, mobile phones, tablets, digital cameras, hard drives, USB sticks and memory cards.

66 See the discussion in Chapter 8 at paragraphs [8.10]–[8.15] and [8.47]–[8.52].

67 Search and Surveillance Act 2012, s 51.

68 See Chapter 4.

69 We discuss this issue below, as overlap with the tracking regime may cause problems in relation to interception as well (see paragraph [9.70]).

- 7.54 Second, a warrant should not be required for data surveillance that solely obtains data that is “publicly available”. For example, the name of a public WiFi network would qualify as an output from an electronic device, but it is visible to anyone in the area who has a WiFi-capable device. We suggest “publicly available” be defined as “generally available to members of the public” (based on a similar definition in the Privacy Act 1993⁷⁰). As we discuss in Chapter 9, this definition would also be relevant in the context of interception.⁷¹
- 7.55 During consultation, DIA expressed concern that our proposed definition of “data surveillance technology” may capture the Digital Child Exploitation Filtering System it operates, which automatically blocks access to known websites that host child sexual abuse images.⁷² We did not have time to explore this. If the filter would otherwise be captured, a specific exclusion should be considered to enable its continued use. Other exceptions to the requirement to obtain a warrant to use data surveillance technology may also be appropriate. The Ministry of Justice should work with enforcement agencies during the development of any amendment legislation to determine whether that is the case.

RECOMMENDATIONS

- R14 The Act should be amended to refer to interception, tracking and visual surveillance “technology” as opposed to “devices”. This will require amendments to section 46 (activities for which a surveillance device warrant is required) and the definitions of “interception device”, “tracking device” and “visual surveillance device” in section 3 of the Act. The definitions should be redrafted in a way that includes the use of computer programs, devices and other technological aids. All references in the Act to “surveillance device warrants” should be replaced with “surveillance warrants”.
- R15 The definition of “visual surveillance device” should be amended to clarify that it includes any device or program that can be used to observe private activity by extrasensory means (for example, thermal imaging and x-ray technology).
- R16 The additional restrictions on visual trespass surveillance in sections 45 and 49(5) should apply to any use of visual surveillance technology to observe private activity in private premises.
- R17 The Act should be amended to enable an enforcement officer to obtain a surveillance warrant to use data surveillance technology. The amendments should include the following:
- (a) Inserting a provision defining “data surveillance technology” as a device, program or other technological aid capable of being used to monitor or record the input of information to, or output of information from, an electronic device. The definition should exclude anything that falls within the definition of “interception technology” or “visual surveillance technology”.
 - (b) Amending sections 45 (restrictions on some surveillance), 49(5) (restrictions on who may apply for specified surveillance warrants) and 50 (approval of law enforcement agencies other than Police to carry out specified surveillance) to apply to the use of data surveillance technology in addition to visual trespass surveillance and interception.

⁷⁰ Privacy Act 1993, s 2 (definition of “publicly available publication”).

⁷¹ See paragraphs [9.12]–[9.18].

⁷² See < www.dia.govt.nz > for more information about the filter.

- (c) Amending section 47 (some activities that do not require a warrant under this Part) to provide that an enforcement officer does not require a warrant to use data surveillance technology:
- (i) to monitor or record inputs or outputs from an electronic device that they are lawfully in possession of; or
 - (ii) in a manner that solely obtains data that is “publicly available”.

R18 A provision should be inserted into the Act defining “publicly available” as “generally available to members of the public”.

SURVEILLANCE FOR NON-EVIDENTIAL PURPOSES

- 7.56 During the course of our review, we became aware of two situations in which surveillance may need to be carried out for purposes other than obtaining evidence of offending:
- To prevent offending or avert an emergency in situations described in section 14(2) (which we refer to here as “emergency” situations). This is where there are reasonable grounds to believe that:⁷³
 - an offence is being committed, or is about to be committed, that would be likely to cause injury to any person, or serious damage to, or serious loss of, any property; or
 - there is risk to the life or safety of any person that requires an emergency response.
 - To locate high-risk offenders who are subject to electronic monitoring and have absconded after tampering with their electronic monitoring device.⁷⁴ By “high-risk offenders”, we refer to offenders who are subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002.⁷⁵

73 Search and Surveillance Act 2012, s 14(2). Section 14 confers warrantless powers on constables to enter a place or vehicle and take any action necessary to prevent the offending or avert the emergency.

74 Electronic monitoring is used to track a person’s whereabouts, to monitor his or her compliance with the conditions of a sentence or order. An electronic monitoring device is attached to the person’s ankle and 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. Electronic monitoring can be imposed on people who are sentenced to community detention (Sentencing Act 2002, s 69E(1)(e)), home detention (s 80C(2)(d)) or intensive supervision (s 54I(3)(f)); as a special condition following a person’s release from a short term of imprisonment (Sentencing Act 2002, s 93); as a special condition following a person’s release from prison on parole or release at the end of a long-term sentence (Parole Act 2002, s 15); people who are subject to extended supervision orders (Parole Act 2002, ss 107K and 15); persons on bail (Bail Act 2000, s 30B); as a special condition of temporary release from custody or temporary removal from prison (Corrections Act 2004, ss 63 and 64); as a special condition of working or being accommodated outside the secure perimeter (Corrections Act 2004, s 65A); or as a condition of an intensive supervision order that is made in respect of a young person (Children, Young Persons, and Their Families Act 1989, s 296J(6)). There are two types of electronic monitoring: Radio Frequency (RF) and Global Positioning System (GPS). RF is mainly used to monitor a person at their detention address. GPS is used to monitor the location of a person whether at home or away from their address.

75 See Chapter 13 at paragraph [13.26] for an explanation of why we propose to treat these types of offenders as “high risk”.

The current powers are inadequate

- 7.57 Surveillance warrants will often be unavailable in the situations identified above, because their issue is predicated on suspicion of an offence and the need to obtain evidential material.⁷⁶ In emergency situations, surveillance will usually be aimed at preventing harmful activity from occurring or at locating a person who is dangerous or whose life is at risk. Where a high-risk offender has tampered with their electronic monitoring device, the primary purpose of surveillance will be to locate them in the interests of public safety. There may not be any relevant evidential material. Even where evidential material is found in the course of the surveillance, that will not usually be the purpose of the surveillance.
- 7.58 Section 48(2)(b) does provide for warrantless surveillance for up to 48 hours in emergency situations, but the availability of that power is dependent on an equivalent warrant power being available. Section 48(1) provides that warrantless surveillance can only be carried out where:
- the enforcement officer is entitled to apply for a surveillance device warrant in the situation covered by the warrantless power; but
 - obtaining a surveillance device warrant within the time in which it is proposed to undertake the surveillance is impracticable in the circumstances.
- 7.59 There is no specific warrantless surveillance power to locate high-risk offenders who abscond after tampering with their electronic monitoring device. While the “emergency situations” power could be engaged in some such cases, the criteria will not always be satisfied. There may not be any specific evidence of a risk to life or safety. A general risk that an offender might be dangerous is unlikely to be sufficient.
- 7.60 There is a further problem. Under section 45 of the Act, the warrantless surveillance powers in section 48 can only be exercised to obtain evidential material in relation to an offence that is punishable by at least seven years’ imprisonment, or certain other specified offences.⁷⁷ Where Police is seeking to locate an offender who is subject to electronic monitoring, the relevant offence (breaching parole conditions or the conditions of an order) does not meet the seven-year threshold.⁷⁸ In emergency situations there may not even be any offence that is being investigated.

Enabling surveillance in emergencies and to locate high-risk offenders

- 7.61 Surveillance may be crucial to ensuring public safety in emergency situations. For example, if a bomb threat is made, visual surveillance of the area at risk (which could include private premises) may allow Police to identify suspicious activity and act to prevent an attack. If a person is missing in circumstances suggesting their life is at risk, tracking their mobile phone may be the only way to find them.
- 7.62 Similarly, there is a clear public interest in locating high-risk offenders due to the threat they pose to public safety. In some cases intercepting their phone calls or text messages may be the only way to locate them.
- 7.63 In our view, it is contrary to the public interest to require the usual warrant criteria to be met in these cases or to apply the seven-year threshold for interception and visual trespass surveillance. It is the risk to safety that justifies the surveillance, rather than the likely existence of evidential material in relation to an offence or the penalty level for that offence.

76 Section 51(a)(ii).

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

78 See, for example, Parole Act 2002, s 71 (the maximum penalty is a one-year term of imprisonment or a fine not exceeding \$2,000).

- 7.64 We recommend that section 48(2) be amended to include a new power for an enforcement officer to carry out warrantless surveillance where they have reasonable grounds:
- to suspect that a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 has tampered with their electronic monitoring device; and
 - to believe that the use of the surveillance technology is necessary to locate them.
- 7.65 In addition, section 51 (which sets out the criteria for obtaining a surveillance warrant) should be amended to enable warrants to be obtained in these cases. We consider this is preferable to simply permitting warrantless powers to be exercised where the enforcement officer would not be entitled to apply for a warrant. That is because warrantless surveillance can only be carried out for 48 hours.⁷⁹ Police told us that an emergency will not necessarily be averted—or an offender may not be located—within that time period. A warrant may therefore need to be sought to enable continued surveillance after the initial 48 hour period expires.⁸⁰
- 7.66 This could be achieved by providing in section 51 that the issuing officer may issue a surveillance warrant if they:
- have reasonable grounds:
 - to suspect that any one or more of the circumstances set out in section 14(2) exist; and
 - to believe that the use of the surveillance technology is necessary to prevent the offending from being committed or continuing, or to avert the emergency; or
 - have reasonable grounds:
 - to suspect that a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 has tampered with their electronic monitoring device; and
 - to believe that the use of the surveillance technology is necessary to locate them.
- 7.67 We also recommend that section 45 be amended to provide that the higher threshold for the use of interception and visual trespass surveillance does not apply to the emergency warrantless power in section 48(2)(b) or to the new warrantless and warrant powers discussed in paragraphs [7.64]–[7.66] above.

⁷⁹ Search and Surveillance Act 2012, s 48(1).

⁸⁰ We note that this is not an issue in relation to the equivalent warrantless search power (s 14), because search powers are not ongoing in the same way as surveillance and are not subject to time limits.

RECOMMENDATIONS

- R19 A new section 48(2)(g) should be inserted to provide that an enforcement officer can carry out warrantless surveillance where they have reasonable grounds:
- (a) to suspect that a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 has tampered with their electronic monitoring device; and
 - (b) to believe that the use of the surveillance technology is necessary to locate that person.
- R20 Section 51 (conditions for issuing surveillance device warrant) should be amended to provide that an issuing officer may also issue a warrant if they have:
- (a) reasonable grounds:
 - (i) to suspect that any one or more of the circumstances set out in section 14(2) exist; and
 - (ii) to believe that the use of the surveillance technology is necessary to prevent the offending from being committed or continuing or to avert the emergency; or
 - (b) reasonable grounds:
 - (i) to suspect that a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 has tampered with their electronic monitoring device; and
 - (ii) to believe that the use of the surveillance technology is necessary to locate that person.
- R21 Section 45 (restrictions on some surveillance) should be amended to provide that the higher threshold for the use of interception and visual trespass surveillance does not apply to the warrantless power in section 48(2)(b) or to the new warrantless and warrant powers outlined in R19 and R20.

Chapter 8

Availability of surveillance powers

INTRODUCTION

- 8.1 In this chapter, we discuss the threshold for exercising surveillance powers, who can exercise surveillance powers and who can issue surveillance warrants. We do not propose any significant changes to the current structure of the Search and Surveillance Act 2012 (the Act).
- 8.2 Two of the issues we address currently only relate to visual surveillance involving trespass and to interception (although they would also be relevant to data surveillance, if our recommendations in Chapter 7 are adopted). A higher threshold must be met before these types of surveillance can be used, which we recommend retaining. We also conclude that the Act should continue to restrict which enforcement officers can use these surveillance methods. However, we do recommend adding Immigration New Zealand to the list of agencies that can be approved to carry out these kinds of surveillance.
- 8.3 Other types of surveillance—tracking and non-trespassory visual surveillance—are not subject to those restrictions. They are, however, only available to enforcement officers who can obtain a search warrant in relation to the offence at issue. We explain that some non-Police enforcement officers are unable to exercise these powers because they only have warrantless powers. We suggest there may be justification for permitting some such enforcement officers to use surveillance powers but note this issue is not restricted to surveillance. It applies to production orders as well. We conclude that further work is required to determine what additional powers are needed and whether they should be included in the Act or other legislation.
- 8.4 Finally, we do not recommend any changes to the current position that only judges (as opposed to other issuing officers) can issue surveillance warrants.

BACKGROUND

- 8.5 As we explained in Chapter 7, surveillance device warrants and search warrants are subject to different rules.¹ Surveillance device warrants must be issued by a judge. In addition, if they relate to visual trespass surveillance or interception, they can only be issued to obtain evidential material in relation to certain serious offences on the application of a constable.
- 8.6 In our Issues Paper, we asked whether surveillance (particularly visual trespass surveillance and interception) is inherently more intrusive than searches, so as to justify its different treatment under the Act.² We noted that, because surveillance is anticipatory and can continue for up to 60 days, it may lead to more personal information being obtained than under a search warrant. It is also necessarily covert, since alerting the target would jeopardise the ongoing surveillance. On the other hand, surveillance can allow an enforcement agency to obtain the information required without physically entering a person's home and searching through their things.

¹ See paragraphs [7.6]–[7.7].

² Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.39]–[3.46] [Issues Paper].

- 8.7 We also noted that, in some cases, the information obtained under a surveillance device warrant is comparable to that which would be obtained under a search warrant.³ Because of this, the different thresholds and requirements applying to some types of surveillance can produce seemingly illogical results. For example, where the threshold for an interception warrant is not met, a text message that cannot be “intercepted” while it is in the course of transmission can nonetheless be obtained shortly after it is received through a search warrant or production order.
- 8.8 We sought submitters’ views on whether all types of surveillance powers (including those relating to visual trespass surveillance and interception) should be:⁴
- able to be exercised in respect of any imprisonable offence;
 - available to any enforcement officer who can apply for a search warrant; and
 - able to be authorised by any issuing officer (rather than only judges).
- 8.9 Finally, we noted that under the Act an enforcement officer can only seek a surveillance device warrant if they could apply for a search warrant in relation to the suspected offence.⁵ Some of the non-Police enforcement agencies who have search powers under other legislation have extensive warrantless powers but no ability to apply for a search warrant. We asked whether surveillance warrants should be available to these enforcement officers.

OFFENCE THRESHOLD

The statutory scheme

- 8.10 Section 45 of the Act states that nothing in Part 3, subpart 1 (surveillance device warrants and declaratory orders) authorises an enforcement officer to undertake trespass surveillance (except by means of a tracking device⁶) or to use an interception device except in order to obtain evidential material in relation to an offence:
- that is punishable by a term of imprisonment of seven years or more;
 - against section 44, 45, 50, 51, 54 or 55 of the Arms Act 1983; or
 - against section 25, 26 or 70 of the Psychoactive Substances Act 2013.
- 8.11 In Chapter 7, we recommended that this higher threshold should also apply to data surveillance if the surveillance regime is expanded to include it.⁷
- 8.12 Section 45 was inserted on the recommendation of the Select Committee that considered the Search and Surveillance Bill. As introduced, the Bill would have permitted all types of surveillance device warrants to be issued in relation to any offence for which the enforcement officer could apply for a search warrant.⁸ However, the Select Committee considered that:⁹

... some forms of surveillance have more effect on privacy than others and should be treated accordingly. It is our view that audio surveillance and the use of visual surveillance devices in

3 At [3.43]–[3.44].

4 At [3.47]–[3.48].

5 At [3.50]–[3.55].

6 In practice, because surveillance device warrants are only available in relation to visual surveillance, tracking and interception (and all interception is covered by s 45 in any case), “trespass surveillance” in this context means visual trespass surveillance.

7 See paragraph [7.50].

8 Search and Surveillance Bill 2009 (45–1), cls 45–46.

9 Search and Surveillance Bill 2009 (45–2) (select committee report) at 4.

circumstances that require enforcement officers to enter private property are intrusions upon privacy which should be authorised only for the investigation of the most serious offending.

- 8.13 The Committee therefore recommended restricting these types of surveillance to the investigation of offences punishable by seven years' imprisonment or more and specified Arms Act offences. The Arms Act offences relate to the unlawful supply, possession or use of firearms in various situations. Their maximum penalties range from a \$4,000 fine or three years' imprisonment at the lower end,¹⁰ to five years' imprisonment at the higher end.¹¹ The Select Committee recommended inserting these provisions into section 45 to "recognise the particular threat that firearms pose".¹²
- 8.14 The Psychoactive Substances Act offences that now appear in section 45 were inserted by that Act. The offences relate to the unlawful manufacture, supply or possession of psychoactive substances.¹³ The maximum penalty for all three offences is two years' imprisonment (for an individual) or a \$500,000 fine (for a body corporate).
- 8.15 Section 45 does not only restrict the issuing of warrants and declaratory orders; it also limits when warrantless surveillance powers can be exercised under section 48 of the Act. Section 48 permits warrantless surveillance in a range of urgent circumstances, including where a person's life or safety is at risk. In order to exercise a warrantless surveillance power involving visual trespass surveillance or interception, an enforcement officer must meet the threshold in section 45 in addition to satisfying the criteria in section 48.¹⁴

Submissions

- 8.16 Around half of the submitters who addressed this question supported making warrants for visual trespass surveillance and interception available in respect of any imprisonable offence to align them with other types of surveillance and searches. The submitters who expressed support were predominantly enforcement agencies. The main reasons given for aligning the thresholds were simplicity and the perceived lack of any principled reason for the distinction. Some submitters expressed doubt that there is any greater privacy interest in respect of a communication during its transmission (which would require an interception warrant to obtain) than after it has been received (which could be obtained under a search warrant or production order). Others argued that surveillance can be less intrusive than a search in some cases. Consistent thresholds would allow enforcement agencies and issuing officers to choose the least intrusive option in the circumstances.
- 8.17 Submitters who opposed lowering the threshold for visual trespass surveillance and interception thought that these methods had the potential to be more intrusive than searches. The New Zealand Law Society and Bell Gully argued that surveillance is more intrusive because it:
- may continue for an extended period of time;
 - is more indiscriminate than searches, resulting in a greater amount of personal and irrelevant information being obtained;

¹⁰ Arms Act 1983, ss 44, 50 and 51.

¹¹ Arms Act 1983, ss 54 and 54. We note that s 54 also includes an offence with a maximum penalty of seven years' imprisonment; however, that would be captured by the general threshold under ss 45(1)(a) and 45(2)(a) of the Search and Surveillance Act 2012 in any case.

¹² Search and Surveillance Bill 2009 (45-2) (select committee report) at 4.

¹³ A psychoactive substance is a substance, mixture, preparation, article, device, or thing that is capable of inducing a psychoactive effect (by any means), but excludes controlled drugs and precursor substances under the Misuse of Drugs Act 1975, alcohol and certain other substances (Psychoactive Substances Act 2013, s 9).

¹⁴ Although we have recommended above that this threshold should not apply in relation to warrantless surveillance in emergency situations: see Chapter 7 at paragraphs [7.56]–[7.67].

- is often intended to obtain evidence of statements or admissions by the target; and
- occurs without the target's knowledge.

8.18 The Law Society thought any extension of surveillance powers should be done on a case-by-case basis by amending section 45 (where specific justification can be provided for using trespass surveillance or interception in relation to a particular type of offence).

Our general view

8.19 We do not recommend that warrants for visual trespass surveillance and interception be available in respect of all imprisonable offences.

8.20 As we explained in our Issues Paper, the Law Commission's 2007 Report, *Search and Surveillance Powers*, recommended that all surveillance should be subject to the same threshold as searches.¹⁵ However, that approach was abandoned during the Bill's passage. The Select Committee considered that visual trespass surveillance and interception were inherently more intrusive than other types of surveillance and should be subject to a higher threshold.¹⁶ Its recommendations reflected submitters' concerns that enforcement officers would receive new surveillance powers that would be disproportionate to the offending likely to be investigated.¹⁷

8.21 The submissions we received did not suggest a radical shift in the level of concern about surveillance activity to justify revisiting this issue. While some enforcement agencies supported changing the thresholds, most of their submissions (with some specific exceptions that we discuss below)¹⁸ did not raise practical problems with the status quo. The submissions we received from legal stakeholders strongly opposed any general change to the thresholds.

8.22 We have some sympathy for their view that extending surveillance powers in reliance on a general principle of consistency carries risks to privacy interests; and that the justification for granting new surveillance powers to investigate other types of offences should be assessed on a case-by-case basis. That approach is consistent with the guidance given by the Legislation Design and Advisory Committee:¹⁹

Search powers should not be granted for the convenience of the agency or ease of prosecution. Each search power must have a separate justification for why it is necessary. A general justification that search powers are required will not be sufficient. The more invasive a particular search power, the greater the justification required to create that search power.

8.23 We do recognise that having a different threshold for some types of surveillance can lead to arbitrary distinctions, which causes frustration for enforcement agencies. However, in our view, that is insufficient in itself to justify what would be a significant expansion of surveillance powers.

The level of the threshold

8.24 The Ministry for Primary Industries (MPI) submitted that the threshold in section 45 should be lowered to five years' imprisonment.²⁰ It considers the seven-year threshold is arbitrary and too

15 Issues Paper, above n 2, at [3.18]–[3.22]; Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.79].

16 Search and Surveillance Bill 2009 (45–2) (select committee report) at 4.

17 At 3.

18 See paragraphs [8.34]–[8.46].

19 *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) at 76.

20 We note that s 45 is not the only barrier to the Ministry for Primary Industries (MPI) carrying out visual trespass surveillance or interception. Section 49(5) or s 50 would also need to be amended to enable this. If s 45 is amended, MPI requested that it be added to the list of "specified law enforcement agencies" in s 50(4) that can be approved to carry out visual trespass surveillance. We discuss this further in paragraphs [8.47]–[8.59].

high. It says that in many of the areas it regulates, offending is difficult to monitor, investigate and prosecute. The ability to use visual trespass surveillance in particular is necessary to enable effective law enforcement.²¹

- 8.25 As we have noted above, the Select Committee that considered the Search and Surveillance Bill recommended that visual trespass surveillance and interception should only be permitted in relation to the “most serious offending”.²² Other pieces of legislation take a variety of approaches to what offences are considered “serious”.
- 8.26 The Sentencing Act 2002 defines “serious violent offence”, for the purpose of engaging the “three-strikes” regime,²³ by reference to 40 specified offences under the Crimes Act 1961.²⁴ The lowest maximum penalty for any of the specified offences is seven years’ imprisonment.²⁵ Similarly, public protection orders can only be imposed where a person has committed a “serious sexual or violent offence”.²⁶ The listed offences are all punishable by at least seven years’ imprisonment.²⁷
- 8.27 In other instances, only offences punishable by 14 years’ imprisonment or more are treated as “serious”. For example, section 15 of the Search and Surveillance Act permits warrantless entry and search to avoid loss of evidence in relation to offences punishable by 14 years’ imprisonment or more. Under the Criminal Procedure Act 2011, a person who has been acquitted of an offence may be subject to further investigation and/or retried only in relation to a “specified serious offence”.²⁸ The definition of “specified serious offence” is limited to offences punishable by imprisonment for life or 14 years.²⁹
- 8.28 In contrast to the provisions discussed above, the Intelligence and Security Act 2017 defines “serious crime” as offences punishable by at least two or three years’ imprisonment, depending on the context.³⁰ Information obtained by an intelligence agency incidentally can be retained and shared with New Zealand Police, the New Zealand Defence Force or another public authority for the purpose of preventing or detecting offences punishable by at least two years’ imprisonment.³¹ Offences punishable by three years’ imprisonment are “serious” for the purpose of determining whether an intelligence agency can collect information about a New Zealander (although there are also other criteria an offence must meet to qualify).³²
- 8.29 Another example of a lower threshold is the definition of “significant criminal activity” in the Criminal (Proceeds) Recovery Act 2009, which covers offences punishable by a maximum term of imprisonment of five years or more.³³

21 See paragraph [8.42].

22 See paragraph [8.12].

23 Sentencing Act 2002, ss 86A–86I.

24 Sentencing Act 2002, s 86A.

25 Crimes Act 1961, ss 191(2), 236(2) and 198(2). The other offences listed in s 86A of the Sentencing Act 2002 are punishable by 10 years’ imprisonment up to life imprisonment.

26 Public Safety (Public Protection Orders) Act 2014, s 7. A public protection order can also be imposed on a person who is subject to an extended supervision order (s 7(1)(b)); however, these are subject to a similarly high threshold (Parole Act 2002, ss 107B and 107I).

27 Public Safety (Public Protection Orders) Act 2014, s 3 (definition of “serious sexual or violent offence”).

28 Criminal Procedure Act 2011, ss 153–154.

29 Criminal Procedure Act 2011, s 152(1).

30 Intelligence and Security Act 2017, s 47 (definition of “serious crime”).

31 Intelligence and Security Act 2017, ss 47 (definition of “serious crime”) and 104.

32 Intelligence and Security Act 2017, ss 47 (definition of “serious crime”), 53 and 58. In addition to being “serious”, the crime must originate or be influenced from outside New Zealand; involve the movement of money, goods or people within a foreign country or from a foreign country to New Zealand or another country; or have the potential to damage New Zealand’s international relations or economic wellbeing (s 58(2)(e)).

33 Criminal Proceeds (Recovery) Act 2009, s 6(1)(a).

- 8.30 These examples demonstrate that there is no consistent approach to what crimes are considered “serious” in statutory terms. However, seven years is a reasonably common threshold and is well within the range of offences that are treated as serious in other legislation.
- 8.31 As we have noted above, we agree that the seven-year threshold is arbitrary.³⁴ A five-year threshold would be as well. There would still no doubt be offences falling just under that penalty line that agencies would argue justify the use of visual trespass surveillance or interception.
- 8.32 Lowering the threshold to five years’ imprisonment would have implications far beyond the legislation administered by MPI. It would open up visual trespass surveillance and interception in relation to a much wider range of offences than is currently the case, including under the Crimes Act. Examples include making a false oath;³⁵ taking, obtaining, or copying trade secrets;³⁶ and wasting or diverting electricity, gas or water.³⁷ No one has suggested to us that the inability to conduct visual trespass surveillance and interception in relation to these types of offences is causing difficulty.
- 8.33 We are not therefore convinced that there is a sufficient basis for departing from the Select Committee’s original view on the appropriate threshold. However, as we discuss below, we do not rule out the possibility of adding further, specific offences to section 45.

Arms Act offences

- 8.34 Some of the more serious offences under the Arms Act 1983 are already listed in section 45 as offences in respect of which visual trespass surveillance and interception can be carried out.³⁸ Police submitted to us that section 45 should be amended to include the following additional offences under the Arms Act:
- Section 16: importing firearms, starting pistols, restricted airguns, or restricted weapons, or parts of firearms, starting pistols, or restricted weapons without permit. (Penalty: \$2,000 fine / one year’s imprisonment.)
 - Section 20: restrictions on possession of firearms (no person shall have a firearm in his possession unless he is of or over the age of 16 years and is the holder of a firearms licence). (Penalty: \$1,000 fine / three months’ imprisonment.)
 - Section 43: selling or supplying firearm or airgun to unlicensed person. (Penalty: \$1,000 fine / three months’ imprisonment.)
 - Section 43A: selling a firearm or ammunition by mail order without a written order endorsed by a member of Police who has inspected the purchaser’s firearms licence. (Penalty: \$1,000 fine.)
 - Section 49A: unlawful possession of firearm or airgun after revocation of firearms licence. (Penalty: \$4,000 / one year’s imprisonment.)
- 8.35 We note that the penalties for these offences are significantly lower than the offences currently listed in section 45. Police acknowledged this, but said that this should not be the determining factor. In Police’s view, any illegal obtaining and possession of firearms is of serious concern, and the current penalties in the Arms Act do not sufficiently reflect this.

34 See paragraphs [8.7] and [8.23].

35 Crimes Act 1961, s 110.

36 Crimes Act 1961, s 230.

37 Crimes Act 1961, s 271.

38 See paragraphs [8.10]–[8.13].

- 8.36 We are reluctant to recommend the inclusion of additional Arms Act offences in section 45 at this stage given the very low penalties currently in place. We are concerned that, if section 45 is amended to list numerous offences that are treated in other legislation as being reasonably low-level, this will undermine the rationale for having a threshold at all.³⁹
- 8.37 We recognise that penalty levels are not the only relevant factor – hence the inclusion of specified offences in section 45, in addition to the general seven-year threshold. Amendments to section 45 may be appropriate where there is a special reason for permitting visual trespass surveillance and/or interception in relation to the offence despite the offence not justifying a higher penalty. As we have discussed, situations where there is a threat to public safety are examples of this, because the risk level is not related to the offence.⁴⁰ However, an analysis of the seriousness of the relevant Arms Act offences and the risks associated with them should be the starting point.
- 8.38 In this context, we note that the Law and Order Select Committee recently conducted an inquiry into the illegal possession of firearms.⁴¹ The Committee considered the penalties for Arms Act offences and recommended they be reviewed. Its report states:
- Several submitters expressed concerns about the penalties under the Arms Act; in particular, that the current penalties have very little deterrent effect.
- We heard that inflation has considerably devalued the financial penalties, reducing the financial hardship imposed on offenders. In addition, New Zealand has low maximum custodial penalties compared with overseas jurisdictions. This is because penalties under the Arms Act are treated as administrative breaches rather than as offences that can carry serious criminal consequences.
- We note that many of the current penalties under the Arms Act are out of date and do not reflect the seriousness of the offences. We recommend that the Government review all of the penalties in the Arms Act, including:
- section 16: importing firearms without a permit
 - section 20: possession of firearms without a licence
 - section 43: selling or supplying a firearm to an unlicensed person
 - section 45: unlawful carrying or possession of firearms, airguns, pistols, restricted weapons, or explosives except for lawful, proper, and sufficient purpose.
- We also propose that if the person committing an offence under the Arms Act is a dealer, the court should treat this as an aggravating factor at sentencing. Dealers have to be particularly held to account because the impact of their offending can have greater consequences than a private owner's non-compliance with the Arms Act.
- 8.39 The Government responded to the Select Committee's report on 14 June 2017.⁴² It has accepted the Committee's recommendation to review the penalties in the Arms Act, agreeing that many of the penalties do not reflect the seriousness of the offences and are overdue for review.⁴³
- 8.40 Following that review, there may be offences for which the penalty will remain below the seven-year threshold but that the Government considers have special features that nonetheless

39 See paragraph [8.20].

40 See paragraphs [7.56]–[7.66].

41 Law and Order Committee *Inquiry into issues relating to the illegal possession of firearms in New Zealand* (I.8A, April 2017).

42 *Government Response to the Report of the Law and Order Committee on its Inquiry into issues relating to the illegal possession of firearms in New Zealand* (J.1, 14 June 2017).

43 At [53]–[56]; Paula Bennett *Government response to firearms select committee report* (press release, 14 June 2017).

justify the use of interception and visual trespass surveillance. If that is the case, amendments to section 45 could be considered alongside any amendments to the Arms Act.

Offences investigated by the Ministry for Primary Industries

- 8.41 In the event that the general seven-year threshold is not lowered, MPI asked us to consider recommending the inclusion of a number of the specific offences it investigates in section 45. These offences are all punishable by five years' imprisonment. They are the most serious offences under the Animal Products Act 1999,⁴⁴ Animal Welfare Act 1999,⁴⁵ Biosecurity Act 1993,⁴⁶ Fisheries Act 1996,⁴⁷ Food Act 2014,⁴⁸ Trade in Endangered Species Act 1986⁴⁹ and Wine Act 2003.⁵⁰ They include, for example, wilful ill-treatment of animals;⁵¹ possession of specimens of endangered, threatened or exploited species;⁵² and deception offences (such as making false or misleading statements) in various regulatory contexts.⁵³
- 8.42 There have been instances of interest groups trespassing on property and making visual recordings in situations where MPI would not be able to undertake visual trespass surveillance under the current requirements in the Act.⁵⁴ The Ministry says this demonstrates that the restrictions in section 45 are hampering its ability to effectively enforce its legislation. It also said that its investigations primarily relate to regulated industries that people choose to operate in, so they arguably have a lower expectation of privacy.
- 8.43 We see some merit in the submission that, where a person chooses to operate in an industry that is regulated, they cannot reasonably expect to have the same level of privacy as they might otherwise. As we discussed in Chapter 2, this is one of the reasons why regulatory agencies have traditionally had broader entry and inspection powers (for the purpose of ensuring compliance with regulatory regimes) than Police.⁵⁵
- 8.44 However, we note that the offences MPI has suggested including in section 45 do not only relate to people in regulated industries. Offences under the Animal Welfare Act 1999, for example, can be committed by any person. This means that, if visual trespass surveillance was permitted in relation to those offences, it could potentially be undertaken in private homes (as opposed to commercial premises). We are not convinced that would be a proportionate response.
- 8.45 In light of this, we have decided that it would be inappropriate for section 45 to permit the general use of visual trespass surveillance in relation to the offences suggested by MPI. However, we do not rule out the possibility that MPI might be able to justify including limited visual trespass surveillance powers in its own legislation. This would allow those powers to be appropriately tailored in a way that cannot practicably be achieved under the Search and Surveillance Act. For example, the ability to conduct visual trespass surveillance could be

44 Sections 126 and 127.

45 Sections 28 and 30A.

46 Section 154O(1)–(15) and an attempt to commit an offence against s 154O(15).

47 Sections 231(1), 231(2), 233, 296B(5) and 296ZC(3)(c).

48 Sections 222, 227, 229 and 230.

49 Section 45(1).

50 Sections 97 and 98.

51 Animal Welfare Act 1999, s 28.

52 Trade in Endangered Species Act 1986, s 45(1).

53 Animal Products Act 1999, s 127; Fisheries Act 1996, ss 231(1), 296B(5) and 296ZC(3)(c); Food Act 2014, ss 227, 229 and 230; Wine Act 2003, s 97.

54 For example, the Farmwatch footage showing treatment of bobby calves on New Zealand farms that was provided to the media and gave rise to MPI investigations (see < www.farmwatch.org.nz > and *Ministry for Primary Industries v Erickson* [2016] NZHC 2635, [2016] NZAR 1553).

55 Chapter 2 at paragraph [2.77].

limited to commercial operators in regulated industries on the basis that their expectation of privacy is lower.

- 8.46 There is some precedent for this approach. The Fisheries Act 1996 already permits entry to any land to use a visual surveillance device in limited situations.⁵⁶ In addition, the Search and Surveillance Act does not confer search powers on non-Police agencies. Those powers are conferred by the other enactments listed in the Schedule. That approach is necessary because the appropriate scope of the search powers varies significantly depending on the context in which the relevant agency operates.⁵⁷ We think there is a strong argument that some surveillance powers will equally need to be context-specific. In such cases, it may be appropriate for surveillance powers to be included in other legislation (although consideration should be given to whether any of the procedural requirements applying to surveillance powers under the Act should be applied, as occurs in relation to search powers).

WHO CAN APPLY FOR SURVEILLANCE WARRANTS

Visual trespass surveillance and interception

- 8.47 Under section 49(5) of the Act, an application for a warrant authorising visual trespass surveillance or interception can only be made by:
- a constable; or
 - an enforcement officer employed or engaged by a law enforcement agency that has been approved by an Order in Council made under section 50.
- 8.48 In Chapter 7, we recommended that this restriction should also apply to data surveillance.⁵⁸
- 8.49 Section 50 provides that a “specified law enforcement agency” can be approved to carry out visual trespass surveillance and/or to use interception devices by Order in Council, on the recommendation of the Minister of Justice.⁵⁹ Before recommending the making of an Order in Council under section 50, the Minister of Justice must consult the Minister of Police and must be satisfied that:⁶⁰
- it is appropriate for the agency to carry out visual trespass surveillance and/or use interception devices;
 - the agency has the technical capability, and the policies and procedures in place, to ensure the safety of people involved in visual trespass surveillance and/or to ensure the reliability and integrity of information obtained through the use of an interception device;
 - where interception approval is sought, the agency has the expertise to extract evidential material in a form that can be used in a criminal proceeding and to present it to the court in an appropriate manner.
- 8.50 A “specified law enforcement agency” is currently limited to the New Zealand Customs Service and the Department of Internal Affairs (DIA).⁶¹ We understand neither of these agencies has sought approval to date.

56 Fisheries Act 1996, ss 199A and 200.

57 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [62].

58 See paragraph [7.50].

59 Search and Surveillance Act 2012, s 50(1).

60 Section 50(2)–(3).

61 Section 50(4).

- 8.51 In practice, an enforcement agency that is not approved to carry out visual trespass surveillance or interception can ask Police to apply for a warrant in relation to the offence (if the offence meets the section 45 threshold). However, whether Police does so will depend on the resources it has available and the extent to which it is prepared to prioritise the request over other investigations.
- 8.52 The restrictions on who can apply for a surveillance device warrant were put in place on the recommendation of the Select Committee. This recommendation followed from the Committee's view that visual trespass surveillance and interception should only be available in relation to serious offences.⁶² The Committee explained:⁶³

The effect of limiting the use of these more intrusive forms of surveillance devices in this way would be in effect to limit which agencies would be permitted to employ these forms of surveillance as currently only the New Zealand Police, New Zealand Customs Service, and the Department of Internal Affairs (in respect of offending under the Films, Videos, and Publications Classification Act 1993) investigate such offending.

However, we consider that as the use of visual surveillance devices in circumstances involving a trespass and of audio surveillance devices is not currently available to non-police agencies, it would be desirable to ensure that these non-police agencies responsible for the investigation of serious offending were required to demonstrate that they had the necessary technical capability and appropriate policies and procedures before being allowed to use such forms of surveillance.

Accordingly, we recommend inserting clauses 45(5) and 45A to ensure that the bill goes further; they provide that the use of visual surveillance devices in circumstances involving a trespass and audio surveillance devices is limited to the police and to a "specified law enforcement agency" that has been approved for the purpose by Order in Council. "Specified law enforcement agency" is defined to mean the New Zealand Customs Service and the Department of Internal Affairs. Accordingly, any extension of these more intrusive forms of surveillance to any other enforcement agencies in the future would require consideration by Parliament. We consider this an appropriate limitation.

Submissions

- 8.53 There was little support for extending surveillance powers to any enforcement officer who can apply for a search warrant. Most submitters considered that the section 50 process for enforcement agencies to obtain approval to carry out visual trespass surveillance and interception was appropriate. If a case could be made to allow more agencies to carry out these activities, that should be done by adding those agencies to section 50 to ensure a managed process.
- 8.54 Bell Gully noted that search warrants are available to many commercial regulators tasked with enforcing laws designed to achieve economic objectives. In its submission, although these are worthy goals, the type of wrongdoing involved is very different from serious criminal offences. A convincing case would need to be made to justify expanding an agency's powers.
- 8.55 Other submitters emphasised the risk of resource duplication if multiple agencies were to develop technical surveillance capabilities; and the importance of ensuring agencies only undertake visual trespass surveillance or interception if they have adequate technical and risk assessment expertise.
- 8.56 One enforcement agency—MPI—supported allowing any enforcement officer to apply for a warrant to carry out visual trespass surveillance or interception. It submitted this would

62 As discussed in paragraphs [8.12]–[8.13].

63 Search and Surveillance Bill 2009 (45–2) (select committee report) at 4–5.

enable enforcement agencies to access communications in real time rather than waiting until a production order can be obtained. In addition, Inland Revenue suggested that permitting enforcement agencies to apply for warrants themselves rather than seeking assistance from Police would be more efficient and effective (although it was unlikely to do this itself). This would allow more investigations to proceed without impacting on Police resources.

Our general view

- 8.57 Because we are not recommending any change to the seven-year threshold in section 45, it will remain the case that only a limited number of agencies are able to investigate offences meeting that threshold. As a result, it would make little sense to enable applications for warrants authorising visual trespass surveillance or interception to be made by any enforcement officer who can apply for a search warrant. In practice, most non-Police enforcement officers would still be unable to seek such warrants in relation to any of the offences they investigate, as section 45 would prevent it.
- 8.58 We have also reached the view that any changes to the agencies that can apply for a warrant should occur through the section 50 process. This will ensure there is proper justification for the agency using visual trespass surveillance and/or interception devices, and that the agency has the appropriate capabilities and expertise in place. The section 50 process—by requiring consultation with the Minister of Police—will also help to ensure coordination between agencies and prevent duplication of resources. For example, Police already has a 24/7 Crime Monitoring Centre to monitor intercepted material. Rather than numerous agencies creating similar centres, it may be more cost-effective to share or build on existing Police capabilities.
- 8.59 We therefore do not recommend any amendment to section 49(5) (except the amendment discussed in Chapter 7 to apply section 49(5) to data surveillance).⁶⁴

Allowing additional agencies to be approved

- 8.60 That leaves the question of whether it is appropriate to enable any additional agencies to seek approval to carry out visual trespass surveillance and interception under section 50.
- 8.61 Immigration New Zealand (Immigration NZ), within the Ministry of Business, Innovation and Employment, asked to be added to section 50 as a “specified law enforcement agency”. It is responsible for investigating and prosecuting people trafficking and smuggling, which are offences under the Crimes Act punishable by up to 20 years’ imprisonment.⁶⁵ It also investigates a number of offences under the Immigration Act 2009 that are punishable by seven years’ imprisonment.⁶⁶ Immigration NZ told us that it is difficult to obtain direct evidence (such as documentary evidence) for some of these offences because part of the transaction may occur offshore. In addition, some of the offences relate to providing false or misleading information to an immigration officer, which will not necessarily involve a “victim” who can give evidence. An ability to carry out interception would assist in obtaining the evidence needed to prosecute these offences.
- 8.62 Section 50 was drafted on the basis that Customs and DIA were the only non-Police agencies that investigated offences that would meet the threshold in section 45.⁶⁷ However, Immigration NZ investigates offences that not only meet the section 45 threshold, but that are (in some cases)

⁶⁴ See paragraph [7.50].

⁶⁵ Crimes Act 1961, ss 98C and 98D.

⁶⁶ Immigration Act 2009, ss 342(1)(b), 343(1)(a), 343(1)(b), 343(1)(c)(i), 345, 348 and 355.

⁶⁷ See paragraph [8.52].

particularly serious. We agree that, given the nature of these offences, surveillance powers are likely to significantly assist in investigating and prosecuting them.

- 8.63 Currently, Immigration NZ undertakes investigations jointly with Police, who can apply for surveillance warrants and provide any technical assistance necessary to execute them. While Immigration NZ indicated it would continue to rely on Police for technical assistance, it saw benefit in being able to apply for surveillance warrants directly. We agree. Immigration officers may have the best knowledge of an investigation, so allowing them to apply for warrants is likely to be a more efficient use of resources. We therefore recommend that Immigration NZ be added to the list of “specified law enforcement agencies” in section 50, to enable it to seek approval to carry out visual trespass surveillance and interception.
- 8.64 We would also not rule out the possible addition of further agencies to section 50 in future, although the justification for that would need to be assessed on a case-by-case basis.⁶⁸

Tracking and non-trespassory visual surveillance

- 8.65 The restriction in section 49(5) on who can apply for a warrant does not apply to tracking and non-trespassory visual surveillance. However, under section 51, a surveillance warrant can only be issued if the suspected offence is one in respect of which the enforcement officer could apply for a search warrant. Only constables can apply for a search warrant under the Act.⁶⁹ As we explained in our Issues Paper, some non-Police enforcement officers have no power to apply for a search warrant under their own governing legislation either.⁷⁰ Instead, they may have extensive warrantless powers. Currently, those enforcement officers are unable to obtain surveillance warrants at all.
- 8.66 For example, park rangers have warrantless powers to search certain vehicles and structures in national parks for evidence of offending,⁷¹ but they have no corresponding ability to apply for a search warrant. This means a park ranger can potentially enter and search a boat without a warrant but cannot obtain a warrant to track the movements of a boat that they have reason to believe will be used to commit an offence.⁷²

Submissions

- 8.67 A majority of submitters who addressed this question (predominantly enforcement agencies) supported allowing enforcement officers with warrantless powers to apply for a surveillance warrant. They saw no rational basis for distinguishing between enforcement officers who have the ability to apply for a search warrant and those with warrantless powers only, given that warrantless powers are only granted in exceptional cases. They thought allowing enforcement officers with warrantless powers to seek surveillance warrants directly rather than going through Police would allow a more efficient use of resources.
- 8.68 One submitter suggested that such an extension should only apply to enforcement officers whose warrantless powers are based on a threshold (such as reasonable grounds to suspect an offence has been committed and to believe evidential material will be obtained), as opposed to regulatory inspection or examination powers.

68 For example, we understand that Inland Revenue investigates some offences under the Crimes Act 1961 (such as ss 258 and 259) that are punishable by 10 years' imprisonment. Although it did not seek to be added to s 50 at this stage, it may wish to do so in future.

69 Section 6(a).

70 Issues Paper, above n 2, at [3.50]–[3.55].

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

72 Examples of relevant offences are removing protected objects (National Parks Act 1980, s 60(1)(d)) and entering specially protected areas (s 13(5)(a)).

- 8.69 The New Zealand Law Society considered that the justification for extending surveillance powers needed to be considered on a case-by-case basis, taking into account the type of offence being regulated, whether surveillance was practically necessary and whether the surveillance would be proportionate to the offence.

Our view

- 8.70 This issue was initially raised with us—and was discussed in our Issues Paper—in the context of surveillance. However, it became apparent during our discussions with enforcement agencies that the issue is a broader one. In order to apply for a production order under the Act, the enforcement officer must be entitled to apply for a search warrant in relation to the documents.⁷³ In addition, some agencies consider the warrantless search powers available to them are inadequate, so they rely on constables to seek search warrants on their behalf. Five agencies indicated that they currently rely on constables to apply for search warrants, production orders and/or surveillance device warrants for them (and there may well be more).⁷⁴ They said that this process can result in significant delays and in some cases may result in investigatory avenues not being pursued.
- 8.71 We deal first with surveillance. In our view, there is likely to be a case for enforcement officers with certain warrantless powers to be able to obtain surveillance warrants.⁷⁵ However, for two reasons, we do not recommend that section 51 be amended to enable a warrant to be issued to any enforcement officer with an applicable warrantless power.
- 8.72 First, we consider any extension of the ability to apply for a surveillance warrant should be limited to where the relevant warrantless power is subject to a “reasonable grounds” threshold. This indicates that the power relates to the investigation of a specific offence, as opposed to being a general inspection power for the purpose of monitoring regulatory compliance. We noted in our Issues Paper that warrantless search powers generally require a high level of justification, as the presumption is in favour of requiring a warrant.⁷⁶ That is true in relation to law enforcement search powers. However, it is not necessarily the case in relation to regulatory powers, which have traditionally been granted in much wider contexts.⁷⁷
- 8.73 Second, as we have explained above, we endorse the approach of extending surveillance powers only where there is specific justification.⁷⁸ We think there is a risk in permitting additional enforcement agencies to apply for surveillance warrants without analysing, in relation to each, whether it is appropriate for them to have surveillance powers and whether they have the necessary expertise and processes in place to do so safely and effectively. Similarly, we think the need for and appropriate scope of any new production powers would need to be considered on a case-by-case basis. It was not possible during the course of this one-year review to undertake that analysis.

⁷³ Search and Surveillance Act 2012, s 71.

⁷⁴ The Department of Conservation, MPI, the Accident Compensation Corporation, the Ministry of Health and the Ministry of Social Development. (The Ministry of Health indicated it does not seek surveillance device warrants, and the Accident Compensation Corporation only seeks search warrants.)

⁷⁵ Because the restrictions in ss 45 and 49(5) would continue to apply, any such warrants could only permit non-trespassory visual surveillance or tracking.

⁷⁶ Issues Paper, above n 2, at [3.55]; 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.

⁷⁷ See the discussion in Chapter 2 at paragraphs [2.75]–[2.80].

⁷⁸ See paragraphs [8.22] and [8.58].

- 8.74 As we have already alluded to,⁷⁹ if production or surveillance powers need to be framed in a way that is specific to the operational context of a particular agency other than Police, it may be more appropriate for that agency to amend their own empowering legislation to include those powers. In our view, the best way forward is for the Ministry of Justice to consult with enforcement agencies to determine which agencies with warrantless powers should be able to apply for a surveillance warrant or production order, and whether that should be provided for in the Search and Surveillance Act or other legislation.
- 8.75 As we have noted above, some agencies also rely on constables to seek search warrants on their behalf because their own search powers are inadequate. As we have explained, only constables are empowered to apply for search warrants under the Act.⁸⁰ The Act did not attempt to incorporate the search powers of other enforcement officers. Those powers remain in the many different enactments listed in the Schedule. In our view, that is appropriate, as the search powers available to non-Police agencies need to be tailored to the specific context in which they operate. If enforcement agencies consider that their search powers are inadequate, that is something they can seek to address through amendments to their own legislation.⁸¹

RECOMMENDATIONS

- R22 Section 50(4) should be amended to add Immigration New Zealand to the list of “specified law enforcement agencies” that may be approved by the Governor-General to carry out visual trespass surveillance and use interception technology.
- R23 The Ministry of Justice should consult with enforcement agencies to determine which agencies with warrantless powers should be able to apply for a surveillance warrant or production order and whether that should be provided for in the Act or other legislation.

WHO CAN ISSUE SURVEILLANCE WARRANTS

- 8.76 The Act provides that a surveillance device warrant may only be issued by a judge (defined as a District Court or High Court judge).⁸²
- 8.77 Only two submitters—both enforcement agencies—supported allowing any issuing officer to issue surveillance warrants. They thought this could help to ensure applications are considered expeditiously. However, neither suggested they had experienced difficulty with the availability of judges in practice.
- 8.78 Most submitters felt that surveillance requires a higher level of oversight because it is a matter of public concern and can involve a substantial intrusion on privacy. They expressed concern that issuing officers who are not judges do not receive sufficient training or have the necessary legal expertise to give proper scrutiny to surveillance device warrants.
- 8.79 In light of the strong opposition to this proposal and the lack of any evidence suggesting there is a problem in practice, we consider the ability to issue surveillance warrants should remain limited to judges.

⁷⁹ See paragraphs [8.45]–[8.46].

⁸⁰ Section 6.

⁸¹ The Ministry of Justice should be consulted on any proposals to create new search powers, and consideration should be given to applying some or all of the provisions in Part 4 of the Search and Surveillance Act 2012 to those new powers.

⁸² Search and Surveillance Act 2012, ss 3 (definition of “judge”) and 53.

Chapter 9

Interception and tracking

INTRODUCTION

- 9.1 In this chapter, we discuss issues relating to the provisions in the Search and Surveillance Act 2012 (the Act) dealing with interception and tracking. We:
- propose amendments to the interception warrant requirement to ensure it applies to metadata and adequately protects privacy interests;
 - discuss the scope of the exception to the requirement to obtain an interception warrant where a party to the communication consents, and recommend amending it to apply to any form of communication (rather than just oral communications);
 - propose that applications for interception warrants be required to include additional information about how the interception will be carried out, in response to issues raised by the Court of Appeal;¹ and
 - recommend changes to the tracking warrant requirement to address practical difficulties encountered by enforcement agencies.

SCOPE OF THE INTERCEPTION WARRANT REQUIREMENT

- 9.2 Section 46 of the Act requires enforcement officers to obtain a surveillance device warrant to use an interception device to intercept a “private communication”.² Interception includes hearing, recording, monitoring or receiving a communication while it is taking place or in transit.³
- 9.3 “Private communication” is defined as follows:

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

¹ *Murray v R* [2016] NZCA 221.

² Search and Surveillance Act 2012, s 46(1)(a). “Interception device” is 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)” but excluding hearing aids.

³ Section 3 (definition of “intercept”).

Issues Paper

- 9.4 In our Issues Paper, we explained the history of the interception regime—which is based on the interception offence in the Crimes Act 1961⁴—and identified some problems that arise as a result of the regime being limited to interception of “private communications”.⁵
- 9.5 By way of brief summary, these were the problems we identified:
- The definition of “private communication” will not be met if any party to the communication “ought reasonably to expect that the communication may be intercepted”. However, if State interception becomes more frequent and that is publicly known, the situations in which members of the public “ought reasonably to expect” interception could significantly increase. In this way the definition is circular.⁶
 - The Act does not allow warrants to be issued to intercept communications that are not “private”.⁷ Such interception will not be an offence under the Crimes Act interception provisions, but may breach the law in other ways. For example, it may involve trespassing on private property to install the device or it could amount to an unreasonable search under section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA). In such cases, enforcement agencies may be unable to carry out the interception at all. Non-private communications may therefore counter-intuitively be afforded greater protection than private ones.⁸
 - Metadata⁹ is unlikely to be covered by the definition of “private communication” because it is a communication between two machines. The definition refers to the parties and their intentions, suggesting it is limited to communications between people. This means a warrant cannot be obtained under the Act to intercept metadata.¹⁰
- 9.6 We sought submitters’ views on whether the interception regime in the Act should be broadened: for example, by requiring a warrant to intercept any “communication” (broadly defined, to include metadata) that is not publicly available.¹¹

Submissions

- 9.7 Roughly half of the submitters who addressed this issue thought that a warrant should be required to intercept any communications that are not publicly available. They noted the distinction between public and private communications is increasingly blurred and thought there should be a presumption that any personal information is protected.
- 9.8 Some enforcement agencies opposed such an approach, arguing there is no expectation of privacy in non-private communications; interception of them will not usually involve trespass;

4 Crimes Act 1961, s 216B.

5 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [4.2]–[4.25] [Issues Paper].

6 See Issues Paper, above n 5, at [4.11]–[4.15]; *Moreton v Police* [2002] 2 NZLR 234 (HC) at [22]; 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).

7 Warrants must be issued in relation to the use of a “surveillance device”, which includes an “interception device”. However, the definition of “interception device” in s 3 is confined to devices “capable of being used to intercept or record a private communication”.

8 Issues Paper, above n 5, at [4.16]–[4.18] and *Moreton v Police* [2002] 2 NZLR 234 (HC) at [29].

9 Metadata is 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 Internet Protocol (IP) addresses the communication was sent and received from. It does not include the content of communications, such as the body of an email.

10 Issues Paper, above n 5, at [4.19]–[4.25]. The Act does permit enforcement officers to require a service provider to provide “call associated data” related to communications that are being intercepted under a warrant (s 55(3)(g)). However, this only covers a limited class of metadata relating to telecommunications (s 55(3)(g) and Telecommunications (Interception Capability and Security) Act 2013, s 3 (definition of “call associated data”). It is also unclear whether this data can be obtained in “real time” or only produced after the fact.

11 Issues Paper, above n 5, at [4.35]–[4.38].

and an enforcement officer should be able to record what they can overhear. However, almost all submitters thought the definition of “private communication” should be amended to ensure that it covers metadata.

- 9.9 In subsequent discussions, New Zealand Police (the only agency that currently undertakes interception) indicated that it did not see a problem with obtaining a warrant to intercept any communications that are not publicly available.¹² The Department of Internal Affairs (DIA) and New Zealand Customs Service emphasised the need to ensure that any amendment did not prevent activities that currently occur pursuant to the tracking regime (as some tracking activity involves “intercepting” location data—such as signals transmitted by mobile phones to cell towers—and DIA and Customs are not currently approved to carry out interception).

A warrant to intercept communications that are not publicly available

- 9.10 For the reasons we set out in our Issues Paper, we think it is important for the Act to require a warrant—and permit warrants to be issued—to intercept metadata.¹³ The fact that the current definition of “private communication” does not appear to cover metadata creates uncertainty for enforcement officers; prevents real-time access to some types of data that could assist in investigations; and has no obvious logical basis given that interception of the *content* of communications (which is likely to contain highly personal information) can be authorised.
- 9.11 We also think that the test for when a warrant is required should not depend on the likelihood of interception. As identified by William Young J in *Moreton v Police* and numerous commentators since, the current focus on whether the particular parties ought reasonably to expect interception may lead to a progressive reduction in privacy rights as surveillance becomes more common.¹⁴ To give an extreme example, if the State decided to intercept the communications of every individual in the country and made this publicly known, arguably those communications would no longer be “private” within the terms of the definition. The observations made by the Supreme Court of Canada in *R v Tessling* (in relation to the reasonable expectation of privacy test) are instructive:¹⁵

In an age of expanding means for snooping readily available on the retail market, ordinary people may come to fear (with or without justification) that their telephones are wiretapped or their private correspondence is being read. One recalls the evidence at the Watergate inquiry of conspirator Gordon Liddy who testified that he regularly cranked up the volume of his portable radio to mask (or drown out) private conversations because he feared being “bugged” by unknown forces. Whether or not he was justified in doing so, we should not wish on ourselves such an environment. Suggestions that a diminished subjective expectation of privacy should automatically result in a lowering of constitutional protection should therefore be opposed. It is one thing to say that a person who puts out the garbage has no reasonable expectation of privacy in it. It is quite another to say that someone who fears their telephone is bugged no longer has a subjective expectation of privacy and thereby forfeits the protection of s. 8. Expectation of privacy is a normative rather than a descriptive standard.

- 9.12 In our view, a better approach is to require a warrant to use interception technology to intercept any communication unless it is “publicly available”. The term “private communication” should be removed. This would increase the objectivity of the inquiry. Whether the particular parties ought to expect interception to be likely would become irrelevant. Instead, the assumption would be that people have a reasonable expectation of privacy in relation to any communication

¹² Subject to the exceptions recognised in s 47 of the Act (for instance, when an officer intercepts a communication they are a party to).

¹³ See above at paragraph [9.5] and Issues Paper, above n 5, at [4.19]–[4.25] and [4.34].

¹⁴ See *Moreton v Police* [2002] 2 NZLR 234 (HC) at [22]; 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).

¹⁵ *R v Tessling* 2004 SCC 67, [2004] 3 SCR 432 at [42].

that they choose to make outside of the public arena. This approach will increase protection of privacy interests and ensure that warrants can be sought in relation to any interception.

9.13 To achieve this, we recommend:

- amending the definition of “intercept” to refer to a “communication” rather than a “private communication”;
- repealing the definition of “private communication”;
- amending section 46(1)(a) to require a warrant to “use interception technology to intercept a communication”; and
- amending section 47 to provide that a warrant is not required to intercept a communication that is publicly available.¹⁶

The existing exceptions to the requirement to obtain a warrant set out in section 47 of the Act would continue to apply.

9.14 We have discussed the definition of “publicly available” above in relation to data surveillance.¹⁷ “Communication” should be broadly defined to include metadata and to provide enough flexibility to cover new forms of communication that may develop. We suggest using the same definition as in section 47 of the Intelligence and Security Act 2017:

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.

9.15 We acknowledge there may be some grey areas in the application of the “publicly available” test. Some degree of ambiguity is unavoidable and necessary to allow the courts to apply the test in a sensible way as technology develops. On balance, we consider the “publicly available” test will be easier for enforcement officers to apply than the “reasonable expectation of privacy” test or the current definition of “private communication”. Under the approach we recommend, the default position would be that a warrant must be obtained whenever interception is carried out, unless it is clear the communication is publicly available.

9.16 The amendments we propose could mean a warrant is required in some situations where a court might find there is no reasonable expectation of privacy. However, we consider the number of such cases is likely to be small. In general, if a communication is not generally available to members of the public, we think the parties should be entitled to expect that it will not be subject to unauthorised State intrusion.

9.17 We acknowledge the concern raised by DIA and Customs that requiring a warrant to intercept metadata might prevent them from carrying out tracking. This can be addressed by clarifying that the tracking regime applies whenever interception is limited solely to location data. We make recommendations to that effect below.¹⁸

9.18 Finally, we note that these proposals would create an inconsistency between the interception regime in the Act and the interception offence in the Crimes Act. However, for the reasons we discussed in Chapter 7, we do not consider this would be unduly problematic.¹⁹

16 This could be combined with the exception for data surveillance discussed above in paragraph [7.54].

17 See paragraph [7.54].

18 See paragraph [9.70].

19 See paragraph [7.26].

RECOMMENDATIONS

- R24 The definition of “private communication” in section 3 should be repealed. Wherever the term “private communication” is currently used, it should be replaced with “communication”. This will require amendments to the definitions of “intercept” and “interception device” in section 3 and to sections 46(1)(a) and 50(3)(a).
- R25 A provision should be inserted into the Act defining “communication” as including “signs, signals, impulses, writing, images, sounds, information, or data that a person or machine produces, sends, receives, processes, or holds in any medium”.
- R26 Section 47 should be amended to provide that a warrant is not required to intercept a communication that is publicly available.

INTERCEPTION WITH CONSENT

- 9.19 The Act recognises some exceptions to the general requirement to obtain a warrant to intercept private communications. Under section 47, a warrant is not required for an enforcement officer to record what they hear while lawfully in private premises, or to carry out “covert audio recording of a voluntary oral communication between 2 or more persons made with the consent of at least 1 of them”.
- 9.20 The basis for the exception being limited to “audio” recordings of “oral” communications is unclear. The Law Commission’s 2007 Report, *Search and Surveillance Powers*, recommended an exception for the “surreptitious recording of a voluntary conversation” (which may be taken to suggest an oral communication) on the basis that this would “reflect the status quo” in the Crimes Act 1961.²⁰ However, under the Crimes Act there is an exception to the interception offence for a person who intercepts any “communication” with the express or implied consent of the originator or intended recipient.²¹ The exception is not limited to oral communications. It is not evident from the legislative history whether the different approach in the Search and Surveillance Act was intentional.

Issues Paper

- 9.21 In our Issues Paper, we explained that the consent exception means a warrant is not required to record a conversation between an informant or undercover officer and a suspect.²² However, this may still amount to a search for the purposes of section 21 of NZBORA²³ or breach other rights, such as the right to refrain from making a statement.²⁴ The admissibility of any evidence obtained may then be challenged on the basis that it was improperly obtained.²⁵
- 9.22 We noted that the approaches taken to consent interception in other jurisdictions vary.²⁶ Australia takes a similar position to ours.²⁷ In the United Kingdom, interception can be carried out with the consent of both or all parties to a communication, or with the consent of only one party if the interception is authorised under the surveillance regime in the Regulation of

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

21 Crimes Act 1961, ss 216A(2) and 216B(2)(a).

22 Issues Paper, above n 5, at [4.39].

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

24 *R v Kumar* [2015] NZSC 124, [2016] NZLR 204.

25 Evidence Act 2006, s 30.

26 Issues Paper, above n 5, at [4.42]–[4.44].

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

Investigatory Powers Act 2000 (UK) (which can often be done by a senior person within the enforcement agency).²⁸

- 9.23 We also outlined some of the arguments for and against the current consent exception.²⁹ The basis for the exception is that interception with one party's consent is no different to that person recalling the conversation and giving evidence as to what occurred.³⁰ The interception simply provides a more accurate record. On the other hand, it can be argued that the other party (or parties) to the communication who are unaware of the interception still have a reasonable expectation of privacy. The State, being subject to NZBORA, should not intrude on that expectation without specific authority.
- 9.24 We asked submitters whether the consent exception should be restricted to where both or all parties to the communication consent, or whether a warrant should be required where the “consenting” party is an undercover officer or other person acting at the direction of an enforcement agency.³¹
- 9.25 We also noted that the fact the consent exception is limited to oral communications causes some practical difficulties for Police. For example, officers cannot intercept abusive text messages being sent to a person who requests the interception.³² We therefore asked submitters whether the consent exception should be amended to apply to all kinds of communications.

Submissions

- 9.26 A majority of submitters opposed restricting the consent exception, on the basis that any party to a communication is free to repeat what they hear and recording prevents later dispute by providing a more accurate record. The submitters who supported amendment considered the consent of one party does not outweigh the privacy interests of the other and submitted a warrant should be required whenever the State is involved in interception.
- 9.27 We also discussed this issue with our Expert Advisory Group. The group unanimously favoured retaining the current consent exception. They suggested that if the exception did not apply where only one party consents, that would encourage undercover officers not to record things to avoid the need to get a warrant. This would make it more difficult for the judge or jury in any subsequent proceedings to determine what occurred if the defence and prosecution disagree. The group also suggested that recordings may benefit defendants as much as—or even more than—prosecutors, as an officer's account may be preferred over a defendant's (particularly if the officer made a contemporaneous written record of the exchange).
- 9.28 There was general agreement among submitters that if the exception is retained, it should apply to all types of communications rather than just oral communications. They saw no principled basis for treating oral communications differently.

Retaining the exception where only one party consents

- 9.29 This issue caused difficulty for us. At a principled level, we are of the view that if one party to a communication consents to its interception without the knowledge of the other parties, those

28 Investigatory Powers Act 2016 (UK), s 44 and Regulation of Investigatory Powers Act 2000 (UK), ss 28, 29 and 32. The United Kingdom's interception offence is also much more limited than in New Zealand. It only applies to interception of communications in transit via a postal service or telecommunications system (Investigatory Powers Act, s 3). This means it is not an offence to use a listening device, including to record phone calls as they are received, although this would still be regulated by the surveillance provisions in the Regulation of Investigatory Powers Act (see *R v Hardy* [2002] EWCA Crim 3012 at [30]–[31] and *R v E* [2004] EWCA Crim 1243, [2004] 1 WLR 3279 at [18]–[32]).

29 Issues Paper, above n 5, at [4.45]–[4.47].

30 See *R v A* [1994] 1 NZLR 429 (CA) at 434, 437, 438 and 448–449.

31 Issues Paper, above n 5, at [4.48]–[4.52].

32 At [4.53].

other parties may continue to have a reasonable expectation of privacy. It follows that, in line with the general principles we see as underlying the Act,³³ authorisation should still be required for that interception.

- 9.30 However, at a practical level we agree with our Expert Advisory Group that discouraging the use of recordings is undesirable. If a person (including an undercover officer) can lawfully engage in a conversation and provide testimonial evidence of it in a subsequent proceeding, the court is likely to be assisted if there is an accurate record of the exchange. For example, in *R v Kumar* the Supreme Court found that a confession elicited by undercover police officers posing as the defendant's cell mates had been obtained in breach of his right to refrain from making a statement.³⁴ The Court undertook a detailed assessment of the interaction between the undercover officers and the defendant (which had been recorded), and concluded it was the functional equivalent of an interrogation.³⁵ The statements were therefore found to have been obtained in breach of the right to refrain from making a statement under section 23(4) of NZBORA, and the evidence was excluded under section 30 of the Evidence Act 2006. The kind of detailed assessment undertaken by the Court in *Kumar* would be much more difficult if the conversation was not recorded.
- 9.31 We can also see the need for the consent exception in other situations where the person consenting to the interception is seeking assistance from enforcement agencies. For example, a victim who is at high risk of serious violence from a former partner may ask Police to intercept their calls or text messages to enable a quick response if the partner indicates they are on the way to the victim's house. In that kind of preventative situation, warrants would not even be available because the criteria for issuing them would not be met.³⁶
- 9.32 On balance, we recommend that the exception should continue to apply where one party to a communication consents. However, we can see potential for interception with the consent of only one party to unreasonably intrude on expectations of privacy in some situations. To help ensure that consent interception is used appropriately, it should be covered by a policy statement.³⁷ This policy statement should also apply to tracking with consent, which we recommend below should be permitted without a warrant.³⁸ The policy statement should include guidance on:
- what amounts to consent and who is capable of consenting (for example, if the person whose communications are to be intercepted is under 14 years of age, the statement might require consent from their parent or guardian);³⁹
 - the procedures that need to be followed to obtain and document consent (for example, it might provide that enforcement officers should explain how the information gathered can be used and where possible obtain the consenting person's written approval);
 - what precautions should be taken before carrying out consensual surveillance (for example, determining whether any third parties who are not under investigation are likely to be impacted by the surveillance, and if so, whether their consent can also be sought without prejudicing the investigation); and

33 Chapter 4 at paragraphs [4.10] and [4.23]–[4.25].

34 *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204. This case is discussed in more detail in Chapter 15 at paragraphs [15.41]–[15.43].

35 At [51]–[67].

36 Search and Surveillance Act 2012, s 51.

37 Policy statements are discussed in Chapter 5.

38 See paragraph [9.63].

39 This would be consistent with the approach taken to consent searches under the Act: see s 95. The Act currently does not set out who can consent to interception.

- any circumstances in which the enforcement officer should seek a warrant despite consent being an option.

9.33 We would encourage use of the warrant procedure if there is any doubt about whether a proposed consent interception may unreasonably interfere with the privacy of non-consenting parties. That could be the case, for example, where the circumstances indicate that the communication will include a significant amount of personal information that is unrelated to the offence under investigation.

Applying the consent exception to non-oral communications

9.34 We consider the consent exception should not be restricted to the recording of oral communications. Section 47(1)(b) should be amended to provide that a warrant is not required for an enforcement officer to “intercept a communication between two or more persons made with the consent of at least one of them”.

9.35 We acknowledge that the rationale of providing a more accurate record of a conversation does not apply to most non-oral communications. Written communications, by their nature, create a permanent record that can be referred to in later proceedings (unless they are destroyed). However, there are some classes of electronic communications that do not create a permanent record. For example, if an undercover police officer knows they are likely to receive Snapchat images incriminating a person they are investigating, Police should be able to intercept those images.⁴⁰

9.36 We can also see value in enforcement officers being able to intercept non-oral communications, such as text messages or emails, at the request of a person who is being targeted by offending. For example, if a person is receiving threats by text message, they may wish to ask Police to intercept their messages to obtain evidence of this.

RECOMMENDATIONS

R27 A provision should be inserted into the Act that requires a policy statement to be issued providing guidance on the use of interception and tracking technology with consent. The statement should include guidance on:

- what amounts to consent, including the procedures for obtaining and documenting consent;
- precautions that should be taken before carrying out consent surveillance; and
- any circumstances in which a warrant should be obtained.

R28 Section 47(1)(b) should be amended to provide that a warrant is not required for an enforcement officer to “intercept a communication between two or more persons made with the consent of at least one of them”.

⁴⁰ Snapchat is a mobile application that allows users to send pictures and videos to each other that are automatically deleted a few seconds after they are viewed. We understand there are ways to take screenshots of Snapchat images in order to preserve them. However, if an undercover officer is in regular contact with associates by Snapchat, this may not be practicable.

INCIDENTAL INTERCEPTION

Issues Paper

- 9.37 In our Issues Paper, we discussed the Court of Appeal’s decision in *Murray v R* in some detail.⁴¹ That decision considered the circumstances in which communications of third parties that are intercepted incidentally in the course of executing a warrant can be used in criminal proceedings. Police officials told us that the decision has caused operational difficulties for them.
- 9.38 In *Murray*, Police had obtained a warrant to intercept the calls of several named individuals who resided at the same address. They proceeded to intercept all calls to and from the landline at that address. In doing so, they intercepted calls not involving the named suspects that were made or received by the wife of one of the named suspects (who also resided at the address). Police sought to rely on these communications in prosecuting a different suspect, Mr Yates, for methamphetamine-related offending.
- 9.39 Mr Yates challenged the admissibility of the evidence on the basis that it was not obtained “in the course of carrying out activities authorised by a surveillance device warrant” as required by section 57(1) of the Act.⁴² The Court rejected the Crown’s argument that Police was justified in intercepting all calls on the phone line because that was operationally inevitable.⁴³ It held that Police should have introduced a step in its process to filter out calls not involving a named suspect by undertaking a preliminary voice identification. The evidence was therefore not obtained “in the course of carrying out activities authorised by a surveillance device warrant”.⁴⁴ However, the Court concluded that the evidence was nonetheless admissible under section 30 of the Evidence Act 2006.⁴⁵
- 9.40 Police told us that this decision is problematic because voice identification of all intercepted calls is not feasible.⁴⁶ Intercepted calls are monitored centrally at a 24/7 Crime Monitoring Centre (CMC). Summaries are provided to the investigating officers, who only listen to calls that appear to be relevant to the investigation. The monitoring of calls is resource-intensive, and Police says it would not be practicable for the investigating officers to perform it. However, CMC employees will not have the necessary knowledge of a given case to carry out voice identification.
- 9.41 In our Issues Paper, we suggested two options for reform that might help to resolve these problems:⁴⁷
- Require applications for warrants to intercept communications to identify:
 - any risk that the communications of a person other than a named suspect will be intercepted; and
 - the process that will be followed to monitor and/or filter intercepted material.
 - Impose a duty on enforcement officers to take all reasonable and practicable steps to minimise the likelihood of intercepting or listening to communications other than those authorised.

41 *Murray v R* [2016] NZCA 221. See the discussion in our Issues Paper, above n 5, at [5.15]–[5.21].

42 Section 57 applies to evidence obtained in the course of carrying out activities authorised by a surveillance device warrant that relates to an offence other than the offence for which the warrant was issued. The section provides that such evidence is “not inadmissible” in criminal proceedings if the offence it relates to is one that a surveillance device warrant could have been issued in relation to.

43 *Murray v R* [2016] NZCA 221 at [151]–[152].

44 At [157] and [163].

45 At [188].

46 Issues Paper, above n 5, at [5.22]–[5.23].

47 At [5.25]–[5.28].

9.42 We sought submitters' views on whether either of these approaches should be adopted.

Submissions

9.43 A majority of submitters supported both of the reform options we suggested. They considered the first option (requiring additional information to be provided in warrant applications) would allow the issuing officer to consider the adequacy of the proposed approach and impose additional conditions if required. A number of enforcement agencies indicated that they already do this as a matter of good practice.

9.44 Some submitters noted that the second option of imposing a duty on enforcement officers would be consistent with the Telecommunications (Interception Capability and Security) Act 2013, which imposes a similar duty on telecommunications providers assisting with interception.

9.45 Although Police did not support either of these proposals in its submission, in subsequent discussions officials indicated the first option would be workable and may help to address the issues raised in *Murray*. They opposed the imposition of a duty on enforcement officers on the basis that it would be unclear what they would need to do to meet the obligation.

Requiring additional information to be included in warrant applications

9.46 We do not propose to impose a duty on enforcement officers to minimise the likelihood of intercepting or listening to irrelevant communications. We agree with Police's concern that the scope of such a duty would be too uncertain and is likely to cause confusion in practice. Listening to irrelevant material will be necessary to some extent in order to identify what material is relevant. However, enforcement officers would need to have regard to the minimal intrusion principle we have recommended including in the Act.⁴⁸

9.47 We have reached the view that applications for warrants to carry out interception should be required to identify:

- any circumstances the enforcement officer is aware of indicating that the communications of third parties may be incidentally intercepted; and
- the process that will be followed to monitor and filter intercepted material.

9.48 We consider these requirements are consistent with the duty of candour on applicants for warrants, which requires disclosure of any information relevant to the question of whether the warrant should be issued.⁴⁹ Including them explicitly in the Act will incorporate best practice into statute and serve as a useful reminder to enforcement officers. It will help to ensure that issuing officers are fully informed of the relevant circumstances and can assess both the proportionality of the proposed interception and whether any conditions are needed to minimise the impact on third parties.⁵⁰

9.49 In the *Murray* case, if the issuing officer had been informed of Police's intention to intercept all calls on the line, they could have: declined to issue the warrant; issued the warrant subject to conditions limiting the scope of the interception that could be carried out under it; or explicitly authorised the interception of all calls on the line. If the latter approach was adopted, the interception of the communications relied on in prosecuting Mr Yates would clearly have been "in the course of carrying out activities authorised by a surveillance device warrant" in terms of section 57(1) of the Act.

48 Chapter 4 at paragraphs [4.57]–[4.68].

49 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [21], referring to *R v McColl* (1999) 17 CRNZ 136 (CA) at 142–143.

50 In line with the principles discussed in Chapter 4.

- 9.50 We do not envisage that the requirements we are proposing would impose a significant burden on enforcement officers. They would not be required to adopt new monitoring or filtering processes as a matter of course. They could simply outline their standard process in the application. For example, a Police application might simply state that the CMC will monitor all calls on a particular line and provide summaries to the investigating officers to allow them to identify relevant communications. In many cases—for example, where the interception relates to a cell phone that is only used by one person—we expect that will be sufficient. In other cases—such as where a number of different people use a landline and not all of them are suspects—the judge may choose to impose additional conditions relating to how the interception is carried out.

RECOMMENDATION

- R29 Section 49 should be amended to require applications for warrants to use interception technology to identify:
- (a) any circumstances the enforcement officer is aware of indicating that the communications of third parties may be incidentally intercepted; and
 - (b) the process that will be followed to monitor and filter intercepted material.

EXCEPTIONS TO THE TRACKING WARRANT REQUIREMENT

- 9.51 The Act requires enforcement officers to obtain a surveillance device warrant 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 ...

- 9.52 Aside from that qualification, the Act does not recognise any exceptions to the requirement to obtain a warrant for tracking. “Tracking device” is defined in section 3:

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

Issues Paper

- 9.53 In our Issues Paper, we explained that the broad definition of “tracking device” captures some types of activity in respect of which enforcement officers suggested they should not be required to obtain a warrant.⁵² The activities we identified were:

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

⁵² Issues Paper, above n 5, at [4.58]–[4.67].

- tracking a thing with the consent of the owner or person entitled to possession (for example, tracking a stolen cell phone at the request of the owner or tracking police cars for safety purposes);
- tracking for search and rescue purposes (for example, tracking a missing person during a rescue operation); and
- using radar to detect the location of vessels or aircraft (including for navigational and collision avoidance purposes).

9.54 Often tracking in these situations is not for the purpose of investigating offending. Because of this, enforcement agencies would not even be able to obtain a warrant because the criteria for issuing them could not be met.⁵³ On the face of the Act, tracking simply cannot be carried out. We asked submitters whether the Act should be amended so that a warrant is not required to use a tracking device in these cases.

Submissions

- 9.55 All submitters who addressed this issue supported amendment to permit warrantless tracking in some circumstances. Though not all submitters addressed all three of the proposed exceptions, no objections were raised to any of them.
- 9.56 Some submitters suggested there should be a more general carve-out in the Act, for example, by providing that use of a tracking device only requires a warrant if it is for law enforcement purposes or to obtain evidential material.

Our general view

- 9.57 We consider that a warrant should not be required to use tracking technology with consent, in emergency situations, or to use radar on ships, boats or aircraft. In our view, recognising specific exceptions to the warrant requirement is preferable to providing a general carve-out for tracking that is not for the purpose of obtaining evidential material. A general carve-out could have unintended consequences, such as permitting enforcement agencies to track people without a warrant for intelligence-gathering or crime prevention purposes.
- 9.58 In relation to emergency situations, we reached the view that the issues raised by enforcement agencies were not limited to tracking. We also considered that, rather than creating an exception to the warrant requirement for emergency situations, it was more appropriate to allow the existing warrantless surveillance power in section 48(2)(b) to be used in more situations. We have addressed this issue in Chapter 7.⁵⁴

Use of radar to locate ships, boats and aircraft

- 9.59 Radar is used on board ships, boats and aircraft for navigational and collision avoidance purposes. It is not only used by enforcement agencies: virtually all large or commercial ships, boats and aircraft (and some smaller ones) use radar. The fact that radar is used as a matter of course is well-known among captains and pilots. Aircraft are also monitored by radar from air traffic control towers. In light of this, we consider that a person who operates or travels on a ship, boat or aircraft has a low expectation of privacy in its location.
- 9.60 In our view, it is unlikely that the use of radar in this way was intended to be captured by the tracking regime. It is unavoidable that enforcement agencies will need to use radar – for example, on Police and Ministry for Primary Industries boats or the Police Eagle helicopter.

⁵³ Search and Surveillance Act 2012, s 51.

⁵⁴ See paragraphs [7.56]–[7.66].

Usually this will not be for the purpose of investigating offending, so a warrant could not be obtained. Nor would it make sense to require a warrant since radar is used as a matter of course. We therefore recommend that section 47 be amended to provide that a warrant is not required to use radar to ascertain the location of ships, boats and aircraft.

- 9.61 This exception would be limited to ocean or air-based use of radar, because different considerations apply in respect of radar use on land. Officials told us that radar cannot currently be used to track vehicles or people on land because features such as buildings or hills would disrupt it. However, should the technology develop in future to enable this, we consider a tracking technology warrant should be required to make use of it. While people expect ships, boats and aircraft to be visible on radar screens, the same cannot be said of vehicles and people on land.

Tracking with consent

- 9.62 The Act provides for warrantless interception where one party consents,⁵⁵ but consent is not an exception to the requirement to obtain a warrant for other types of surveillance.
- 9.63 Where tracking is concerned, enforcement agencies drew our attention to a number of problems that result from the lack of a consent exception. A stolen cell phone cannot be tracked at the request of the owner, and enforcement officers (or vehicles they operate) cannot be tracked for safety purposes with their consent. We see no reason for requiring a warrant in these cases. Tracking, compared to interception, is far less likely to affect third parties. We therefore recommend that, if consent is obtained from the person being tracked, or from the person entitled to possession of the thing being tracked, no warrant should be required.
- 9.64 In our discussion about consensual interception, we recommended that the Act require a policy statement to be issued providing guidance on the use of consent surveillance.⁵⁶ That statement should also cover tracking with consent. We explained what that statement should contain in paragraph [9.32] above. In relation to tracking, there may be particular value in seeking consent from, or notifying, any third parties who might be affected by the tracking. For example, if a police car is tracked we would expect any officers who use it to be informed of that.

A broader consent exception?

- 9.65 We considered whether consent should be a general exception to the warrant requirement, applying to all types of surveillance. However, where visual surveillance and data surveillance are concerned, we think a consent exception could be problematic.
- 9.66 Consent interception is limited to communications involving the consenting person. This can be achieved, for example, by concealing a recording device on the consenting person. Visual surveillance is more difficult to confine and is generally of an area. Would that mean that, if a person living in a flat consented to visual surveillance, the flat could be monitored 24/7 even when the consenting person is not present?
- 9.67 Similar issues could arise in relation to data surveillance. Like visual surveillance, data surveillance technology may be difficult to confine to a particular person. It will generally gather all data (or particular types of data) input into or emitted by a device. Where there are multiple users of a device, third parties may be affected even when they are not interacting with the consenting person.

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

56 See paragraphs [9.32]–[9.33].

- 9.68 Enforcement agencies did not raise the lack of a consent exception for visual surveillance as a problem. Nor could we think of specific examples where consensual data surveillance might be useful.⁵⁷ Given this and the potential difficulties identified above, we do not recommend a broad consent exception applying to all types of surveillance. However, if enforcement agencies can demonstrate a need for a wider consent exception and there is a way to ensure the surveillance is sufficiently targeted (for example, by requiring consent from all users of a device or all residents of a property), we express no firm view against it.

RECOMMENDATION

- R30 Section 47 should be amended to provide that a warrant is not required for an enforcement officer to:
- (a) use radar to ascertain the location of ships, boats or aircraft; or
 - (b) track a person with their consent or track a thing with the consent of the person entitled to possession of it.

RELATIONSHIP BETWEEN TRACKING AND OTHER SURVEILLANCE

- 9.69 This issue was not raised in our Issues Paper but has come to our attention during the review. There are situations where the tracking regime in the Act overlaps with other types of surveillance and with production orders. This creates difficulty for enforcement agencies, as it is unclear what kind of warrant or order they need to obtain. It is particularly problematic where tracking overlaps with another kind of surveillance (such as interception) that is subject to the higher threshold in section 45.
- 9.70 In our view, if technology that might otherwise fall within the definition of “interception technology” or “data surveillance technology” will be used in a way that solely generates location data, the enforcement officer should only need to obtain a warrant authorising the use of tracking technology. If any additional information will be obtained, an interception or data surveillance warrant would be required. We think that is consistent with the policy decision made by Parliament that tracking is less intrusive than interception.⁵⁸ Provided no additional data is obtained, the kind of technology used to carry out the tracking should not alter that. That conclusion is reinforced by the fact that the current definition of “tracking device” focuses on the outcome (ascertaining location) rather than the nature of the technology used.
- 9.71 In addition, the definition of “tracking technology” should exclude the use of visual surveillance technology. If devices such as video cameras or thermal imaging devices are used to track a person’s location, that should be dealt with under the rules around visual surveillance. We think that is necessary because of the difficulty in determining when a visual surveillance device is being used to “help ascertain the location of a thing or person”. Virtually any visual surveillance could be seen as having that effect, since it gives a visual representation of people and things that will necessarily disclose their location.
- 9.72 Excluding the use of visual surveillance technology from the definition of “tracking technology” would mean that a warrant is not required if the observation is in a public place or in the curtilage of private premises for under three hours. However, as we discuss in Chapter 11,

⁵⁷ Although, as we have noted above at paragraph [7.55], further work will be needed to determine what exceptions to the requirement to obtain a warrant for data surveillance are appropriate.

⁵⁸ Chapter 8 at paragraph [8.12].

visual surveillance not requiring a warrant would still need to be conducted in accordance with a policy statement.

- 9.73 Finally, the Act should clarify that enforcement officers can obtain location data after the fact pursuant to a production order and no surveillance warrant is required for this purpose. For example, cell phone tower data could be obtained from a service provider indicating a person's whereabouts at a particular time in the past. Currently, enforcement agencies indicated they are uncertain whether they require both a surveillance warrant and a production order in this situation. We see no reason for requiring both, since the thresholds for tracking and for obtaining production orders are the same. Whether a tracking technology warrant or production order is more appropriate will depend on the circumstances (in particular, whether the data is required in real time).
- 9.74 We note that, under the current definition of "tracking device", we would not expect a request for location data under a production order to qualify in any event. That is because an enforcement officer will not generally use a "device" to ascertain location when they seek data from a service provider under a production order. However, if the definition is extended to "tracking technology", the position may become less clear. We see benefit in clarifying the position to avoid any doubt.

RECOMMENDATIONS

- R31 A provision should be inserted into the Act stating that an enforcement officer can use tracking technology that also falls within the definition of "interception technology" or "data surveillance technology" under a warrant or power authorising the use of tracking technology only, provided that it will be used in a manner that solely generates location data.
- R32 The definition of "tracking technology" should exclude the use of visual surveillance technology.
- R33 The Act should be amended to include a provision stating that an enforcement officer can obtain location data after the fact pursuant to a production order and that no surveillance warrant is required for this purpose.

Chapter 10

Surveillance: procedural matters

INTRODUCTION

- 10.1 In this chapter, we deal with three discrete issues raised with us by enforcement agencies that relate to how surveillance powers are executed and how the information obtained through surveillance is dealt with. We recommend amendments to the Search and Surveillance Act 2012 (the Act) to:
- clarify that a warrant can authorise enforcement officers to enter properties near a target property in order to execute a warrant without being detected;
 - permit enforcement officers to re-enter a property that has been the subject of surveillance after the warrant has expired to remove a surveillance device; and
 - permit enforcement agencies to retain “raw surveillance data” (such as surveillance camera footage or audio recordings) that contains evidential material.
- 10.2 These issues were raised with us and discussed in our Issues Paper in the context of surveillance. However, as we explain below, we have since become aware that the first issue relates to the execution of search warrants as well. Our recommendations on that issue are therefore of broader application.

ENTRY TO THIRD-PARTY PREMISES

The statutory scheme

- 10.3 The Act does not explicitly address the extent to which enforcement officers can enter premises other than those that are the target of surveillance (“third-party premises”) in order to install a surveillance device.
- 10.4 Section 55(3) of the Act requires a surveillance device warrant to specify:
- (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: ...
- 10.5 It is unclear whether the “premises” referred to in section 55(3)(h)(i) are limited to the target premises described in section 55(3)(d) or whether they can also include third-party premises. The Law Commission’s 2007 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”.¹ However, it is not clear from the

¹ Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [11.103].

legislative history of the Search and Surveillance Bill whether that was Parliament’s intent. The phrasing “any” premises suggests it may have been, but there is room for doubt.

- 10.6 In addition, the Act does not set out what procedures apply where a third party’s property is entered. For example, it does not state whether the third party must be notified of the entry.

Issues Paper

- 10.7 We explained in our Issues Paper that enforcement officers may need to cross third-party premises in order to enter the target premises without detection.² For example, if the target premises 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 it from the back.
- 10.8 We suggested that, if it were considered appropriate for enforcement officers to cross third-party premises in some situations, the Act should specifically provide for this.³ By comparison, the Australian surveillance legislation permits “the entry, by force if necessary, onto the premises, and onto other specified premises adjoining or providing access to the premises”.⁴
- 10.9 We also pointed out that any entry to third-party premises will impact on the privacy of persons who are not suspected of any wrongdoing (although in most cases the intrusion will be reasonably low-level).⁵
- 10.10 We sought submitters’ views on whether the Act should provide for entry to third-party premises; whether the premises to be entered and the reason for the entry should be specified in the warrant application; and whether the persons executing the warrant should be required to notify the occupiers of the third-party premises (unless it would prejudice the investigation).⁶

Submissions

- 10.11 All of the submitters who addressed these questions supported amending the Act to specifically provide for entry to premises other than the target premises. All but one submitter thought the premises to be entered should be specified in the warrant, rather than the Act conferring a general statutory power to enter third-party premises.
- 10.12 Around three-quarters of submitters who addressed the issue thought that the occupiers of the properties in question should be notified of the entry, unless the grounds for deferring notice in section 131(2) are met (that is, if notification would endanger the safety of any person, prejudice the successful exercise of the entry and search power, or prejudice ongoing investigations).
- 10.13 One submitter drew our attention to the fact that this issue is not limited to surveillance. Search warrants can also be executed covertly in some situations.⁷ In those cases, there may also be a need to cross third-party premises in order to access the property to be searched without detection.

Requiring warrants to specify additional premises that may be entered

- 10.14 We agree that this issue is not limited to surveillance. In fact, the problem is more pronounced in relation to search warrants. That is because the search warrant provisions, unlike the

² Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [5.4] [Issues Paper].

³ Issues Paper, above n 2, at [5.6].

⁴ Surveillance Devices Act 2004 (Cth), s 18(2)(a)(ii).

⁵ Issues Paper, above n 2, at [5.8].

⁶ At [5.9].

⁷ Search and Surveillance Act 2012, s 134.

- surveillance warrant provisions, do not confer a power on enforcement officers to enter “any premises, area, or vehicle specified in the warrant”. Instead, an enforcement officer is only permitted to enter the place, vehicle or other thing that the person is authorised to enter and search.⁸
- 10.15 Entry to third-party premises may be crucial to allow a search or surveillance power to be exercised safely and without prejudicing an ongoing investigation. We think it is important that the Act provides for it, to ensure that enforcement agencies can perform their functions effectively.
- 10.16 We recommend that applications for search warrants and surveillance warrants, and the warrants themselves, should be required to specify any third-party premises that may be entered. The proposed entry would need to be necessary to carry out the search or surveillance authorised by the warrant without endangering the safety of any person or prejudicing ongoing investigations.
- 10.17 However, we are conscious of the impact any such entry will have on third parties. Enforcement agencies told us that in most cases an entry to third-party premises will be fleeting and only curtilage will be crossed. But there may be other cases where the entry is more substantial: for example, enforcement officers may need to spend several hours on a neighbouring farm watching the target property and waiting for the occupiers to leave.
- 10.18 In either case, if the occupiers of third-party premises are unaware that enforcement officers are about to enter, it is entirely possible that the enforcement officer will intrude on private activity. Even a fleeting entry across a person’s backyard might involve an enforcement officer overhearing a private conversation or seeing a person sunbathing. In order to minimise the impact on third parties’ privacy, we think it is appropriate that they be notified of the entry before it occurs wherever possible.
- 10.19 That approach is consistent with the general presumption in the Act, which favours notification to occupiers unless it would prejudice the investigation.⁹ The case for notification is arguably even stronger where third parties are concerned, since there are no grounds for suspecting them of any wrongdoing that might justify the invasion of privacy.
- 10.20 We have therefore reached the view that the requirements in sections 131(1)(a), 131(2) and 131(4)–(7) for enforcement officers to identify themselves before entry or leave a notice for the occupier should apply with any necessary modifications where an enforcement officer enters third-party premises. Sections 134–135 should also apply, allowing the identification and notice requirements to be deferred by a judge if providing notice would endanger the safety of any person or prejudice ongoing investigations.
- 10.21 The identification and notice requirements should only apply if the entry to third-party premises would amount to a trespass. This would mean, for example, that enforcement officers do not need to locate and notify the occupier where the land (although being privately owned) is open to public use.
- 10.22 Enforcement agencies expressed concern that a third party who is notified of an entry might alert the person who is under investigation. They were also concerned that they might have to disclose the reason for the entry, which would have privacy implications for the person under investigation.

⁸ Section 110(a).

⁹ See ss 131–135. Notification is not required for surveillance as a matter of course because it will always need to be carried out covertly. However, a judge can order that a person be notified after surveillance has ceased (s 61(1)(c)).

- 10.23 We are not convinced that either of those concerns justifies not providing notice, although the former may affect the timing of the notice. As to the first concern, we consider it just as likely—if not more likely—that a third party will alert the person who is under investigation if they are not notified of the entry in advance and discover enforcement officers on their property. If enforcement officers notify the third party, they can explain that they are authorised to carry out the search or surveillance covertly, and that any disclosure may prejudice the investigation and/or constitute an offence.¹⁰ Where there is some specific reason to believe that a third party will alert the target (for example, if they are known to be close friends), notice could be deferred.
- 10.24 We see no need for enforcement agencies to explain to a third party who they are investigating and why. We consider that, to avoid any additional intrusion on the privacy of the target, enforcement officers should simply tell the third party that they are authorised, by virtue of a warrant, to cross the property to allow for the warrant to be executed.

RECOMMENDATION

R34 The Act should be amended to allow an issuing officer, when issuing a search warrant or surveillance warrant, to authorise entry to premises other than the premises that are the subject of the search or surveillance (third-party premises). The amendments should include the following:

- (a) Inserting a provision that states an issuing officer may authorise entry to third-party premises where they are satisfied the entry is necessary to carry out the authorised search or surveillance without endangering the safety of any person or prejudicing ongoing investigations.
- (b) Providing that sections 131(1)(a), 131(2), 131(4)–(7) and 134–135 (which contain identification and notice requirements) apply with any necessary modifications where an enforcement officer enters third-party premises. The enforcement officer should explain that they are authorised to cross the property in order to execute a warrant, but should not be required to show the occupier a copy of the warrant or disclose any details about the investigation. The identification and notice requirements should only apply if the entry to third-party premises would amount to a trespass.

REMOVAL OF SURVEILLANCE DEVICES

The statutory scheme

- 10.25 The Act requires surveillance device warrants to state that entry onto premises is permitted in order to remove a surveillance device.¹¹ 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.

Issues Paper

- 10.26 In our Issues Paper, we explained that the inability to re-enter premises to remove a surveillance device after a warrant has expired is problematic.¹² In order to avoid detection and ensure their

¹⁰ It appears possible that disclosure would in some cases amount to an offence under s 117(e) of the Crimes Act 1961 (wilfully attempting to obstruct, prevent, pervert or defeat the course of justice): see *R v Harn* HC Rotorua T021771, 23 October 2002.

¹¹ Section 55(3)(h).

¹² Issues Paper, above n 2, at [5.11]–[5.12].

safety, enforcement officers may need to wait some time for an opportunity to enter premises. This may not occur before a warrant expires.

- 10.27 We sought submitters' views on whether the Act should provide for removal of devices after a warrant expires. We noted that most comparable regimes in New Zealand and overseas provide for the removal of devices after a warrant expires pursuant to a further "removal" or "retrieval" warrant.¹³ Another option would be to provide a statutory re-entry power.
- 10.28 We identified one key advantage that a removal warrant would have over a statutory re-entry power.¹⁴ It would allow an issuing officer to consider any known changes in circumstance that might affect how the re-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 and remove the device rather than entering the premises covertly.

Submissions

- 10.29 All submitters who addressed this question supported providing for removal of surveillance devices after a warrant expires. One submitter noted that removal of devices will ensure surveillance does not continue inadvertently.
- 10.30 Most submitters thought that the Act or the original warrant should permit entry to remove a device within a certain period. A removal warrant could then be obtained if removal was unable to be effected within that timeframe.

Permitting removal of surveillance technology after a warrant expires

- 10.31 We agree that the Act should permit re-entry to premises after a surveillance warrant expires to remove surveillance technology. While enforcement agencies should aim to remove surveillance technology before expiry, we accept that will not always be possible. In relation to gang headquarters in particular, which may be heavily guarded, re-entry may need to be carefully planned.
- 10.32 The Act should provide for an initial statutory re-entry period. If re-entry can occur soon after the warrant expires, the likelihood that circumstances will have significantly changed will be reasonably low. We recommend that the Act permit re-entry to premises to remove surveillance technology within 21 days after the expiry of the warrant that permitted its installation. However, if the enforcement officer is aware of a significant change in circumstances (for example, that the occupiers have changed) or the 21-day period expires, the Act should require a removal warrant to be sought from a judge.
- 10.33 A removal warrant could be issued if the judge is satisfied that the warrant is necessary in the circumstances.¹⁵ A warrant may not be necessary, for example, if the re-entry could realistically be done by consent without prejudicing an ongoing investigation. The judge would be able to impose conditions setting out how the re-entry should occur. A warrant could be valid for up to 21 days, and a further warrant could be issued in relation to the same premises if required.

13 See Intelligence and Security Act 2017, s 85; Criminal Code RSC 1985 c C-46, s 186(5.2); Surveillance Devices Act 2004 (Cth), ss 22–26.

14 Issues Paper, above n 2, at [5.15].

15 We note this is the same basis on which removal warrants can be issued under the Intelligence and Security Act 2017.

RECOMMENDATION

- R35 The Act should be amended to provide for the removal of surveillance technology following the expiry of a surveillance warrant. The following provisions should be inserted:
- (a) A provision permitting an enforcement officer to re-enter premises without a warrant to remove surveillance technology within 21 days after the expiry of the warrant that permitted the installation of the device. This power should not apply if the enforcement officer is aware of a significant change in circumstances (such as a change in occupation of the property).
 - (b) A provision empowering a judge to issue a removal warrant authorising re-entry to a property to remove surveillance technology if they are satisfied that the warrant is necessary in the circumstances. The judge should be able to impose conditions setting out how the re-entry should occur.
 - (c) A provision stating that removal warrants are valid for a period of 21 days, but that a further removal warrant may be issued in relation to the same premises if required.

RETENTION OF RAW SURVEILLANCE DATA

The statutory scheme

10.34 The Act places restrictions on the retention of raw surveillance data by enforcement agencies. Raw surveillance data is defined in section 3:

raw surveillance data—

- (a) means actual video recordings or actual audio recordings; and
- (b) includes full transcripts, or substantial parts of transcripts, of audio recordings

10.35 Raw surveillance data can be retained:¹⁶

- until any criminal proceedings have been concluded (and any appeal rights have been exhausted); or
- for a maximum of three years, if criminal proceedings have not been commenced but the data is required for an ongoing investigation.

10.36 After that period, raw surveillance must be deleted unless it forms part of the court record (which will not usually be the case¹⁷) or—if proceedings have not been commenced—if an order is obtained from a judge permitting retention for a further period.¹⁸ Judges can only order retention of raw surveillance data for a maximum of two additional years and must be satisfied that retention is required for the purpose of an ongoing investigation.

10.37 However, a judge can order indefinite retention of *excerpts* from raw surveillance data if satisfied that they may be required for a future investigation.¹⁹ Enforcement agencies can also retain, without any judicial order, information obtained from raw surveillance data that

16 Search and Surveillance Act 2012, s 63(1).

17 The court record is only required to contain certain documents relating to the formal steps taken in a proceeding (Criminal Procedure Rules 2012, r 7.2). It does not include the evidence given at trial so is unlikely to include raw surveillance data in most instances.

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

19 Section 63(3)–(4).

does not itself constitute raw surveillance data if it may be relevant to an ongoing or future investigation.²⁰

Issues Paper

- 10.38 In our Issues Paper, we noted enforcement agencies had expressed concern that the requirement to delete raw surveillance data could cause difficulty where cases are reopened or defendants are retried at a much later date.²¹ Relevant evidence may no longer exist.
- 10.39 We explained that the requirement to delete raw surveillance data was inserted into the Search and Surveillance Bill on the recommendation of the Select Committee. The Committee's concern was that raw surveillance data may include a large amount of material that is not evidential and that relates to people who are innocent of any offending.²²
- 10.40 We also noted that the rules around raw surveillance data are different to those applying to other types of investigatory materials. For example, forensic copies of data held in a computer system or data storage device can be retained indefinitely and in their entirety if they contain some evidential material.²³
- 10.41 We sought submitters' views on whether the Act should be amended to permit the retention of raw surveillance data that is evidential material and any associated information that, if removed, would compromise the integrity of the evidential material.

Submissions

- 10.42 All but one of the submitters who addressed this question agreed the Act should provide in some way for retention of raw surveillance data that might be required in future for evidential purposes. New Zealand Police officials made the point, in discussions with us, that raw surveillance data may be exculpatory. Its destruction may therefore be detrimental to defendants who are later retried.
- 10.43 The New Zealand Criminal Bar Association opposed amendment as it thought that the risk of the data being inappropriately accessed outweighed any benefits that retention would bring if a case is reopened or a defendant retried at a later date.

Permitting retention of raw surveillance data for evidential purposes

- 10.44 The intention of the Select Committee in inserting the destruction requirement does not appear to have been to require destruction of evidential material. Rather, the concern was about the retention of large amounts of irrelevant material, particularly where it relates to people who are innocent of any offending. We consider this concern can be addressed while still ensuring that relevant evidential material is retained in case it is required in subsequent proceedings.
- 10.45 Police has assured us that raw surveillance data is stored securely and is subject to strict controls on who can access it. The risk of inappropriate access to raw surveillance data is therefore low. We also agree with the submission made by Police that destruction of raw surveillance data may be detrimental to a defendant. Raw surveillance data may contain exculpatory evidence

²⁰ Section 63(6).

²¹ Issues Paper, above n 2, at [5.32].

²² Search and Surveillance Bill 2009 (45-2) (select committee report) at 6.

²³ Search and Surveillance Act 2012, s 161(2). The term "computer system" is defined in s 3 of the Act 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.

that would be relevant in a retrial. The deletion of raw surveillance data containing evidential material therefore carries greater risk than its retention.

- 10.46 As we have noted, in our Issues Paper we suggested that the Act could permit the retention of raw surveillance data that is evidential material and any associated information that, if removed, would compromise the integrity of the evidential material. As a result of our consultation with enforcement agencies, we no longer think that would be practicable. It would require enforcement agencies to sort through all raw surveillance data to determine what is “evidential material”. Given the amount of raw surveillance data that may be generated during a surveillance operation (which can last up to 60 days),²⁴ that would be an extremely resource-intensive exercise. We are not convinced the cost of that exercise would be justified. It would also be difficult for enforcement officers to anticipate which data may become relevant in a subsequent proceeding (and therefore what qualifies as “evidential material”).
- 10.47 Instead, we propose that raw surveillance data should be dealt with in the same way as forensic copies. If the investigating officer determines that the raw surveillance data obtained in relation to a particular target does not contain any evidential material, it would need to be destroyed. Otherwise, the data relating to that target could be retained in its entirety.
- 10.48 By “target”, we refer to the person, place, vehicle or thing specified in the warrant under section 55(3)(d) or the description of the surveillance provided under section 55(4). A single warrant may relate to multiple targets (for example, several people who are suspected of involvement in joint offending). Focusing on each target separately, as opposed to all data obtained under a particular warrant, will ensure that the data relating to a particular target is destroyed if no evidential material is found (even if evidential material is found in relation to other targets covered by the same warrant).
- 10.49 This approach will ensure that all of the relevant information is available in the event of subsequent proceedings. However, it should still go a long way towards achieving the Select Committee’s goal of protecting people who are not under suspicion by requiring deletion of data that contains no evidential material.
- 10.50 We note that, if there are still concerns about the impact of retention on people’s privacy, one option would be to consider placing restrictions on how material retained by enforcement agencies can be accessed and used (through statutory rules and/or a policy statement).

RECOMMENDATION

R36 Sections 63–64 (which relate to the retention and disposal of raw surveillance data) should be repealed and replaced with a provision that states the following:

- (a) An investigating officer must delete raw surveillance data obtained in relation to a target if they determine that it does not contain any evidential material. “Target” should be defined as a person, place, vehicle or thing specified in the warrant under section 55(3)(d) or a description of the surveillance provided under section 55(4).
- (b) If raw surveillance data obtained in relation to a target is a mixture of evidential material and data that is not evidential material, it can be retained in its entirety.

²⁴ Section 55(1)(c).

Chapter 11

Public surveillance

INTRODUCTION

- 11.1 In Chapter 5, we recommended that chief executives of enforcement agencies be required to issue policy statements in relation to certain classes of activity that are generally lawful but have the potential to intrude on reasonable expectations of privacy. This included the following classes of activity:
- the use of visual surveillance technology in circumstances not requiring a surveillance warrant (“public visual surveillance”);
 - accessing social media platforms to obtain information about individuals or classes of individuals (“social media monitoring”); and
 - observation or monitoring of an individual’s movements or activities in a manner not requiring a surveillance warrant (“directed surveillance”).
- 11.2 These three classes of activity can be described (in broad terms) as types of “public surveillance”. We use that term to refer to the monitoring or observation of people, places, things or information that either occurs in public places or relates to information that is publicly available. This is not a precise term or one that we recommend defining in the Search and Surveillance Act 2012 (the Act). We simply use it here for ease of reference.¹
- 11.3 Because the types of public surveillance referred to above are generally lawful and can be accessed without a warrant, they can provide valuable information to enforcement agencies prior to or in the early stages of investigations. They may allow agencies to identify geographic areas or groups of people of potential concern, in order to target crime prevention and detection efforts. They may also be used to undertake preliminary inquiries in relation to specific individuals, in order to determine whether there are sufficient grounds to obtain a warrant to use more intrusive search or surveillance methods.
- 11.4 In this chapter, we discuss why some public surveillance—despite its public nature—may still impact on the privacy of individuals; explain why we consider policy statements are an appropriate way to address privacy concerns; and examine more closely the three classes of activity listed above. We then discuss the kind of guidance we envisage these policy statements containing.
- 11.5 At the end of this chapter, we address the position in relation to activity that can occur in public but involves the disclosure of information that is not generally available to members of the public (for example, the use of a drug detector dog to discern the contents of personal luggage). The Act currently does not specifically enable the use of this type of activity for general crime detection or prevention purposes (for example, screening all luggage at train stations for the presence of drugs)² and it may amount to an unreasonable search under section 21 of the

1 Indeed, some of the activities we discuss in this chapter might better be described as a “search” where they are carried out in a targeted way or on a “one-off” occasion rather than for general screening or monitoring purposes. We discuss this further in paragraph [11.75].

2 Although it may be permitted in legislation conferring powers on certain non-Police enforcement officers (see the Customs and Excise Act 1996, ss 137 and 172).

New Zealand Bill of Rights Act 1990 (NZBORA). We explain why we do not propose any amendments to permit this in the absence of a specific search or surveillance power.

THE CURRENT LEGAL FRAMEWORK

- 11.6 Public surveillance is not explicitly addressed by the Act. Instead, its use is currently governed by a combination of case law, section 21 of NZBORA, general provisions in the Act, the principles in the Privacy Act 1993 and internal policies.

Case law and section 21 of NZBORA

- 11.7 There is some case law supporting the proposition that State actors have the same powers as members of the public, except to the extent that the exercise of those powers is circumscribed by statute, would conflict with legislation or the common law or would breach protected rights.³ This principle has been applied by the Court of Appeal in determining the legality of surveillance carried out in public places. In *Lorigan v R*, the Court held that covert video surveillance conducted in public was lawful because “there was no statutory or common law prohibition of such activity and it would not have been unlawful for a citizen to do the same thing”.⁴ On that approach, the use of public surveillance by enforcement officers will generally be lawful where the officer does no more than what a private citizen could do.
- 11.8 However, as McGrath J noted in *Ngan v R*, “the residual freedom of officials is constrained by the Bill of Rights Act. Residual freedom to act can never justify a breach of protected rights”.⁵ Public surveillance has the potential to intrude on reasonable expectations of privacy so as to amount to a “search” under section 21. For example, in *Lorigan*, the Court found that the use of one particular surveillance camera that had night-vision capability did amount to a “search” because it could capture images that could not be seen by the naked eye.⁶
- 11.9 Where public surveillance would amount to a search, it must be carried out reasonably in order to avoid breaching section 21. As we discussed in Chapter 4, proportionality lies at the heart of the reasonableness assessment.⁷ A court will consider whether “the public interest in being left alone by government must give way to the government’s interest in intruding on the individual’s privacy in order to advance its goals, notably those of law enforcement”.⁸

The Search and Surveillance Act

- 11.10 Where an enforcement officer is uncertain about whether proposed public surveillance would amount to a search and, if so, whether it would be reasonable, they could seek a declaratory order. However, as we discussed in Chapter 6, declaratory orders can only authorise the use of an investigatory method in a particular case. They may be valuable where an agency wishes to use a new, untested method and there is significant doubt about whether it would amount to an unreasonable search in terms of section 21 of NZBORA. But enforcement officers could not be expected to obtain a declaratory order every time they wish to undertake public surveillance,

3 *Minister for Canterbury Earthquake Recovery v Fowler Developments Ltd* [2013] NZCA 588, [2014] 2 NZLR 587 at [82]–[83], referring to the judgments of McGrath J in *Ngan v R* [2007] NZSC 105, [2008] 2 NZLR 48 at [93]–[100] and *Rogers v Television New Zealand Ltd* [2007] NZSC 91, [2008] 2 NZLR 277 at [110], and Tipping J in *Ngan* at [45] and *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [217]. Compare the contrary view of Elias CJ in *Hamed* at [24]. This point was left open on appeal in *Quake Outcasts v Minister for Canterbury Earthquake Recovery on appeal from Minister for Canterbury Earthquake Recovery v Fowler Developments Ltd* [2015] NZSC 27, [2016] 1 NZLR 1 at fn 152.

4 *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [29]. The Supreme Court declined leave to appeal this decision in *Lorigan v R* [2012] NZSC 67.

5 *Ngan v R* [2007] NZSC 105, [2008] 2 NZLR 48 at [97] per McGrath J.

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

7 Chapter 4 at paragraph [4.46].

8 *R v Jefferies* [1994] 1 NZLR 290 (CA) at 319 per Thomas J, referring to *Hunter v Southam Inc* [1984] 2 SCR 145 at 159–160.

given the routine activities this can include (such as a police officer watching a person in a public place or looking at a public Facebook profile).

- 11.11 Where a proposed activity does not give rise to a sufficiently significant level of concern on the part of the enforcement officer to seek a declaratory order, in most cases, it is carried out without any specific authorisation or guidance under the Act. In theory, a surveillance warrant could be issued for some types of public surveillance, but this is not required.⁹

Privacy principles and internal policies

- 11.12 The principles in the Privacy Act apply to any agency that collects or holds personal information, including enforcement agencies.¹⁰ By way of brief summary, the following principles are particularly relevant in the context of public surveillance:¹¹

- *Principle 1:* personal information should not be collected by an agency unless the collection is necessary for a lawful purpose connected with a function or activity of the agency.
- *Principle 2:* personal information must be collected directly from the individual concerned.
- *Principle 3:* where an agency collects personal information directly from the subject, they must take reasonable steps to ensure that person is aware of a number of matters, including the fact that the information is being collected and the purpose of the collection.
- *Principle 4:* an agency must not collect personal information by means that are unlawful, unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.
- *Principle 5:* an agency that holds personal information must take such security safeguards as are reasonable in the circumstances to ensure the information is protected from loss, unauthorised access or other misuse.
- *Principle 9:* an agency must not hold personal information for longer than is required for the purposes for which the information may lawfully be used.
- *Principle 10:* an agency that holds personal information that was obtained in connection with one purpose must not use the information for any other purpose.
- *Principle 11:* an agency that holds personal information may only disclose it in certain specified situations, such as where disclosure is connected to the purpose for which the information was obtained or is authorised by the individual the information relates to.

- 11.13 The application of these principles is subject to certain exceptions. In particular, principles 2, 3, 10 and 11 need not be complied with if it would prejudice the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.¹²

- 11.14 Some enforcement agencies have internal policies on their use of some types of public surveillance, based on the principles in the Privacy Act. For example, New Zealand Police has an internal policy on the use of CCTV cameras that is published on its website.¹³

9 For example, the Act appears to permit warrants to be issued in relation to any use of a visual surveillance device (s 3 definition of “surveillance device”, and s 55(3)(c)) even though they are only required where the surveillance observes private activity in private premises (or on the curtilage of private premises for over three hours in a 24-hour period or eight hours in total) (s 46).

10 Privacy Act 1993, ss 2 (definition of “agency”) and 6. “Personal information” is any information about an identifiable individual: s 2 (definition of “personal information”).

11 Privacy Act 1993, s 6. Although we acknowledge there may be room for debate about whether covert surveillance amounts to “collection” of information: see Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at [3.7]–[3.11].

12 Privacy Act 1993, s 6, principles 2(2)(d)(i), 3(4)(c)(i) and 10(c)(i).

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

11.15 With the exception of principle 6, which entitles a person to access personal information about them, the privacy principles do not give rise to legal obligations that are enforceable in the courts.¹⁴ If evidence is obtained in a manner that breaches the principles, that may be relevant in assessing whether the evidence was obtained unfairly for the purpose of section 30 of the Evidence Act.¹⁵ However, it is unlikely to be determinative. As a majority of the Supreme Court said in *R v A*:¹⁶

... while we accept the possibility that the fact that personal information was obtained in breach of the privacy principles will be relevant under s 30, we think it unlikely that it will be of any independent significance in many instances. This is because what will be significant to the s 30 assessment is the nature of the conduct at issue rather than the fact that it constitutes a breach of the privacy principles. For the sake of completeness, we should also note that compliance with the privacy principles does not eliminate the possibility that the information at issue may be found to have been improperly obtained for the purpose of s 30.

11.16 The Privacy Act does provide a complaints process where a person believes the privacy principles have been breached. The Privacy Commissioner can investigate any action that is or appears to be an interference with the privacy of an individual and seek to reach a settlement between the parties.¹⁷ If the matter cannot be resolved, proceedings may be commenced in the Human Rights Review Tribunal.¹⁸ If the Tribunal is satisfied on the balance of probabilities that an agency has interfered with the privacy of an individual, it may grant relief (including a declaration, orders directing or restraining action and/or damages).¹⁹

PUBLIC SURVEILLANCE AND EXPECTATIONS OF PRIVACY

11.17 In Chapter 2, we explained that protection of privacy in the search and surveillance context was historically equated with protection of property rights.²⁰ However, during the 1990s the courts began to recognise that section 21 of NZBORA protects a broader range of privacy interests. It is now well-established that State action will be treated as a “search” under section 21 if it intrudes on reasonable expectations of privacy.²¹ Trespassory conduct is not required.²²

11.18 This broader approach to what amounts to a search is reflected in the Search and Surveillance Act. The Act requires enforcement officers to obtain a warrant before using tracking, visual surveillance and interception devices in certain situations, many of which may not involve any trespass.²³ For example, a warrant is required to carry out visual surveillance of private activity on the curtilage of private premises for over three hours in a 24-hour period or eight hours in total.²⁴ This kind of visual surveillance can often be carried out using a device situated on public property. Similarly, warrants are required to use tracking devices even though the tracking may occur entirely in public places.²⁵

14 Privacy Act 1993, s 11.

15 *R v A* [2017] NZSC 42 at [38].

16 At [40].

17 Privacy Act 1993, s 69.

18 Privacy Act 1993, s 82.

19 Privacy Act 1993, s 85.

20 Chapter 2 at paragraphs [2.17]–[2.18].

21 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [163]; *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22].

22 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [164].

23 Search and Surveillance Act 2012, s 46.

24 Search and Surveillance Act 2012, s 46(1)(e).

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

11.19 The recognition that section 21 protects broader privacy interests than just property interests is particularly important in the context of technological developments. Technology increases the potential for surveillance to be carried out by reducing the natural constraints previously imposed by resource limitations. As Alito J observed in *United States v Jones* (where the United States Supreme Court held that the installation of a GPS²⁶ tracking device on a car was a “search” under the Fourth Amendment):²⁷

In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.

11.20 As we have noted, the Act already recognises the high level of intrusion involved in certain types of surveillance and requires a warrant to conduct them. However, there are other types of surveillance for which no warrant is required that may nonetheless intrude on reasonable expectations of privacy in some cases. This will not always be an easy line to draw. Whether public surveillance intrudes on reasonable expectations of privacy may depend on a number of factors, including the following:

- Whether observation of a person is “casual” or involves “intensive scrutiny” (such as undercover officers following and photographing a person over an extended period).²⁸ While a person cannot control who observes them in a public place, they may still expect not to be personally identified and subject to extensive surveillance.²⁹
- Whether technology is used to enable observation of something that could not otherwise be seen by an enforcement officer (for example, by using a night-vision camera).³⁰
- Whether the surveillance, despite occurring in a public place, observes private activity (for instance, if a drone flying in public airspace is used to observe what is occurring in a private back yard).³¹
- Whether the surveillance involves making a permanent record of the activity observed (and the length of time for which any record is stored).³²

11.21 Public surveillance may also raise unique considerations in the context of determining whether any intrusion on privacy is reasonable. As we observed in our Issues Paper:³³

26 Global Positioning System (GPS) is a satellite navigation system used to determine the ground position of an object or person.

27 *United States v Jones* (2012) 132 S Ct 945 at 963. The Fourth Amendment is the United States equivalent of s 21 of the New Zealand Bill of Rights Act 1990. It provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”.

28 Melvin Gutterman “A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance” (1998) 39 Syracuse L Rev 647 at 706 (cited with approval in *R v Wise* [1992] 1 SCR 527 at 558 per La Forest J and *R v Spencer* 2014 SCC 43, [2014] SCR 212 at [43]–[44]).

29 *R v Wise* [1992] 1 SCR 527 at 558 per La Forest J.

30 *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [25]; *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [164].

31 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [168] per Blanchard J: “if, in order to see into or carry out surveillance of such a private space, it were necessary to climb up on a fence or place a camera up a power pole, for example, that action is likely to constitute a search”. The Act recognises this concern to an extent by requiring a warrant to observe private activity on the curtilage of private property, but only where the observation exceeds three hours in a 24-hour period or eight hours in total (s 46(1)(e)). While it would be impracticable to require a warrant for all observations of a shorter duration, they may still intrude on reasonable expectations of privacy in some cases.

32 Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis, Wellington, 2015) at [18.11.12] (citing *Peck v United Kingdom* app no 4647/98, 28 January 2003 at [57], *PG & JH v United Kingdom* app no 44787/98, 25 September 2001 at [57] and *R v Liu* [2015] NZHC 732 at [171]).

33 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.108] [Issues Paper].

Public surveillance ... 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.

- 11.22 The fact that public surveillance is not directed at the investigation of a specific offence and/or affects a large number of people is likely to be relevant to the proportionality assessment underlying section 21.³⁴

CONSULTATION

Issues Paper

- 11.23 In our Issues Paper, we sought submitters' views on which, if any, types of public surveillance should be covered by the Act and how the Act should address them. We discussed two kinds of public surveillance methods:³⁵

- those that are already used but are not subject to specific regulation in a law enforcement context (such as CCTV and social media monitoring); and
- those that are not in general use because there is significant doubt about whether they would amount to an unreasonable search under section 21 of NZBORA (for example, the use of drug detection dogs or chemical residue detectors to screen people and bags for drugs in public places).

Neither of these types of methods is specifically addressed in the Act.

- 11.24 We observed that public surveillance can be an important law enforcement tool, particularly in helping enforcement agencies to prevent or respond to threats to public safety. On the other hand, depending on the manner in which it is conducted, it may impact on the privacy of large numbers of people – many of whom may not be suspected of any wrongdoing. If it is widely used to monitor the population at large, it may also have a chilling effect on freedom of expression. We noted that the use of CCTV, in particular, is now subject to statutory regulation in a number of jurisdictions.³⁶
- 11.25 We suggested that regulating public surveillance in some way could help to ensure it is only used where there is a demonstrable law enforcement need that outweighs the public interest in being free from undue State interference. However, we indicated that a warrant process was unlikely to be appropriate given the ongoing and generally lawful nature of public surveillance activity, and the fact that it is often not targeted at specific offending. We suggested statutory criteria or policy statements setting out the circumstances in which public surveillance can legitimately be used might be a better approach.

Submissions

- 11.26 Submitters were roughly evenly split on whether the Act should attempt to deal with public surveillance at all. Enforcement agencies were generally opposed to regulation. They submitted the principles in the Privacy Act were sufficient to address the use of public surveillance; there is a low expectation of privacy in public places; and any greater regulation would hinder

³⁴ See paragraph [11.9] and Chapter 4 at paragraphs [4.44]–[4.56].

³⁵ Issues Paper, above n 33, at [3.104]–[3.129].

³⁶ At [3.119]. Regulation is particularly common in European countries. The examples we referred to were the United Kingdom, Spain and Sweden.

effective law enforcement. However, Police suggested amending the Act to include powers enabling general screening for illicit drugs and/or dangerous items such as firearms in specific public places (such as domestic airports and maritime ports³⁷).

- 11.27 The submitters who supported regulation thought that public surveillance may intrude on reasonable expectations of privacy, particularly if it targets a particular individual. The New Zealand Law Society agreed that warrants were unlikely to be suitable for forms of public surveillance not targeting individuals. However, it suggested the Act could usefully set out some principles or criteria applying to the use of public surveillance by enforcement agencies: for example, that it must meet a demonstrable law enforcement need, be proportionate to the aims of the surveillance and must comply with the provisions of the Privacy Act. The submissions did not address in any detail the extent to which particular types of public surveillance should or should not be regulated.

POLICY STATEMENTS FOR PUBLIC SURVEILLANCE

- 11.28 We have concluded that the Act should require the Commissioner of Police and the chief executives of relevant enforcement agencies to issue policy statements on the following types of public surveillance:

- public visual surveillance;
- social media monitoring;
- directed surveillance.

- 11.29 We set out our reasons for that conclusion below, discuss each of these specific types of public surveillance in more detail and explain what information the policy statements would need to contain.

There is a need for clear, consistent and transparent guidance

- 11.30 As we have discussed above, it is clear that some instances of public surveillance may intrude on reasonable expectations of privacy. Depending on the manner in which public surveillance is conducted and the justification for its use in particular circumstances, it may breach section 21 of NZBORA. In addition, in the absence of clear guidance on the use of public surveillance, there is a risk that widespread monitoring of the general population by the State will become routine. In our view, that is to be avoided. The free expression of opinions and exchange of information is one of the fundamental underpinnings of a democratic society.³⁸ If members of the public feel their communications and activities are being monitored by the State, they may feel constrained in expressing potentially controversial political, religious or ideological views.³⁹
- 11.31 We do not consider the principles in the Privacy Act provide sufficient protection against unjustified public surveillance. The principles are not specifically designed to address law enforcement activity. They are necessarily framed at a high level of generality. While they provide a helpful starting point, they are not a substitute for more detailed guidance. The effect

37 Customs officers can already screen a person or their luggage for prohibited items when they disembark from or are about to embark onto an international flight or sailing: see ss 29, 32 and 149–149A of the Customs and Excise Act 1996.

38 Butler and Butler, above n 32, at [13.6.8]–[13.6.13].

39 A number of studies support the view that government surveillance has a chilling effect on individuals' expression and access to information. See, for example, Elizabeth Stoycheff "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring" (2016) 93 *Journalism & Mass Communication Quarterly* 296; Jonathon Penney "Chilling Effects: Online Surveillance and Wikipedia Use" (2012) 31 *Berkeley Tech L J* 117; United States Department of Commerce National Telecommunications & Information Administration "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities" (13 May 2016) < www.ntia.doc.gov > .

of the principles in a particular context and the steps that must be taken to ensure they are complied with are unlikely to be obvious to enforcement officers. The Office of the Privacy Commissioner agreed there would be benefit in more specific guidance for enforcement agencies in the context of public surveillance.

- 11.32 Enforcement agencies already have some internal policies relevant to the use of public surveillance. We would encourage this practice, but we do not think it adequately addresses the risks associated with public surveillance. Agencies are not required to have policies on particular activities; whether or not they do is entirely at their discretion. Nor are there any standard consultation processes to ensure that agencies' internal policies reflect a consistent government position on what is lawful and reasonable. In addition, although some policies are published,⁴⁰ this is not required or done consistently. We think it is important that, where there is significant potential for State intrusion on individuals' privacy, the practices adopted by enforcement agencies are transparent and accessible to the public.

Policy statements are an appropriate mechanism

- 11.33 In our view, a warrant regime would be inappropriate for public surveillance. Much of the activity that would fall within the public surveillance methods we discuss below will not intrude on reasonable expectations of privacy. For instance, it could include an enforcement officer simply walking down the street and observing people walking past. Even where reasonable expectations of privacy are engaged by public surveillance, there will be classes of cases in which its use will almost always be reasonable. Requiring warrants to conduct public surveillance in all cases would be impracticable and a waste of State resources.

- 11.34 We also consider that creating specific statutory rules about the circumstances in which various public surveillance methods can be used is not viable. As we discussed in Chapter 4, it is impossible to delineate with precision the circumstances in which reasonable expectations of privacy will or will not exist.⁴¹ That is particularly true in an area where technological developments are constantly changing the landscape. Any statutory rules are likely to become quickly outdated. The following observation of McGrath J in *Ngan v R* is particularly apt in the case of public surveillance:⁴²

Requiring prior parliamentary authority generally or in relation to certain types of actions can in theory provide desirable democratic legitimacy, and also better legal certainty, but there are logistic difficulties in making that approach work. Codification of all government power would be a huge task and, if attempted, many powers would inevitably be so broadly expressed as to make the democratic advantages illusory.

- 11.35 We have therefore reached the view that public surveillance is most appropriately addressed through the policy statement regime, which we discussed in Chapter 5. Both the principles we have recommended including in the Act and those in the Privacy Act would inform those statements. The policy statement process would ensure enforcement officers have clear guidance on how the relevant principles apply in the context of specific types of public surveillance they may wish to conduct in the course of their work. The consultation requirements for policy statements will help to achieve consistent guidance across government (to the extent appropriate) that accurately reflects the current law. The guidance will be available to the public, providing transparency and accountability for government practices.

40 For example, New Zealand Police *Crime Prevention Cameras (CCTV) in Public Places Policy* (May 2010).

41 Chapter 4 at paragraphs [4.17]–[4.18].

42 *Ngan v R* [2007] NZSC 105, [2008] 2 NZLR 48 at [96].

- 11.36 The key benefit that policy statements would have over statutory rules is flexibility. This is particularly important for public surveillance, since the activity concerned is lawful. We would not wish to impose undue constraints on the everyday activities of enforcement agencies, thereby reducing their effectiveness. Policy statements will be able to be updated as required to deal with changes in technology or to provide guidance on new situations that arise.
- 11.37 As we recommended in Chapter 5, policy statements could also be issued in relation to any additional classes of activity that the Commissioner of Police or chief executive of the relevant agency considers appropriate. This may be particularly useful in the context of public surveillance. It may, for instance, be appropriate to issue additional policy statements covering the use of new types of public surveillance as technology and investigatory methods develop.
- 11.38 Policy statements would work in tandem with declaratory orders. We would still expect enforcement officers to apply for declaratory orders if they have significant doubts about the lawfulness or reasonableness of a proposed activity (for example, because the relevant policy statement does not clearly address it). Policy statements themselves should include guidance on when it will be appropriate for an enforcement officer to seek a declaratory order.
- 11.39 As we explained in Chapter 5, policy statements would only relate to activity that is lawful. They could not authorise unlawful activity. Exclusion of evidence or NZBORA claims may still result if an enforcement officer acts in accordance with a policy statement that does not accurately reflect the law.

Public visual surveillance

- 11.40 By “public visual surveillance”, we refer to any use of visual surveillance technology that would not require a warrant under the Act. This will be the case where the surveillance occurs in a public place and does not involve:⁴³
- observation and/or recording of private activity in private premises; or
 - observation and/or recording of private activity in the curtilage of private premises for more than three hours in a 24-hour period or eight hours in total.
- 11.41 The most obvious examples of public visual surveillance are the use by enforcement officers of CCTV cameras or body-worn cameras in public places. However, it would also include visual surveillance from drones and helicopters (provided any observation of private activity on curtilage does not exceed three hours). As we discussed in Chapter 7, “visual surveillance technology” would (under our proposals) also include technologies that permit extrasensory observation – such as thermal imaging and x-ray. These activities would also be covered by the policy statement to the extent that they do not require a warrant. For example, use of thermal imaging by the Police Eagle helicopter to track fleeing offenders should be included.
- 11.42 Finally, the policy statement on visual surveillance should cover the use of any specific adjuncts to or applications of visual surveillance technology. Examples include automatic number plate readers and the use of facial recognition technology in conjunction with CCTV cameras to identify people.
- 11.43 Visual observation not using technology—for instance, where a police officer observes a suspect in a public place—is discussed below under “directed surveillance”.⁴⁴

⁴³ Search and Surveillance Act 2012, s 46.

⁴⁴ See paragraph [11.64] and following.

Why public visual surveillance should be subject to policy statements

- 11.44 In many cases, public visual surveillance will not intrude on reasonable expectations of privacy. As Blanchard J observed in *Hamed v R*, “[p]eople 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”.⁴⁵ However, public visual surveillance can raise significant privacy concerns where it allows enforcement officers to obtain information of a nature or in a form that is qualitatively different from what an ordinary observer would discern.
- 11.45 In paragraph [11.20] above, we referred to four factors that may influence whether public surveillance constitutes an intrusion on reasonable expectations of privacy. Public visual surveillance has the potential to engage all of these factors, depending on the manner in which it is carried out.
- 11.46 First, public visual surveillance can allow people to be identified and subjected to intensive scrutiny that would not ordinarily be anticipated in a public place. This could be the case where networks of CCTV cameras are set up, allowing enforcement agencies to track individuals’ movements and activities, particularly if this is paired with facial recognition software to identify those individuals.⁴⁶ This is an example of technology allowing information to be gathered and analysed at a rate that could not—in practical terms—be achieved by enforcement officers on the ground. If such practices became commonplace, it would “spell the end of the ‘practical obscurity’, that many people take for granted when they move about in public”.⁴⁷
- 11.47 Second, public visual surveillance may involve the use of technology that enables the observation of something that could not otherwise be seen by an enforcement officer or by a member of the public. The example already recognised in New Zealand case law is night-vision cameras.⁴⁸ The use of x-ray to scan luggage or people in public places or CCTV cameras to read text messages on mobile phones⁴⁹ would likely raise even more significant privacy concerns.
- 11.48 Third, public visual surveillance may be used to observe private activity. Drone use is likely to raise particular issues because it could allow enforcement agencies to capture activity occurring in areas that are not ordinarily visible by members of the public. Because drones are not as loud as helicopters, the people being observed may be unaware of it.
- 11.49 Fourth, public visual surveillance may involve making a permanent record of an activity that might otherwise be promptly forgotten. This creates potential for the record to be inappropriately accessed and used at a later date. The authors of *The New Zealand Bill of Rights Act: A Commentary* suggest that, although “unregulated and by-chance observation” of a person in public is not a search for section 21 purposes:⁵⁰

... that position should not necessarily be definitive if the observation is conducted 24 hours a day by permanently installed video cameras. That is because the facility to make a permanent record of activities observed on a video, and to store the activities recorded indefinitely, raises a significantly

45 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [167].

46 As we noted in our Issues Paper, facial recognition is already in common use by Police in the United States: Issues Paper, above n 33, at [3.115]–[3.116]. See Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law, 2016).

47 Rachel Levinson-Waldman “Hiding in plain sight: a Fourth Amendment framework for analyzing government surveillance in public” (2017) 66 Emory LJ 527 at 549.

48 *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [25]; *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [164].

49 Shabnam Dastgheib “Powerful surveillance cameras read texts” *Stuff* (online ed, Wellington, 3 May 2012). We note this is unlikely to qualify as “interception” because the text message would no longer be “in transit”.

50 Butler and Butler, above n 32, at [18.11.12] (citing *Peck v United Kingdom* app no 4647/98, 28 January 2003 at [57], *PG & JH v United Kingdom* app no 44787/98, 25 September 2001 at [57] and *R v Liu* [2015] NZHC 732 at [171]).

more serious potential threat to personal privacy, which may well call for some sort of control through a “reasonableness” standard.

- 11.50 Finally, public visual surveillance will, in many cases, affect a large number of people not under suspicion. As we have noted above, this may impact on the proportionality of its use in particular instances and therefore whether that use is reasonable.⁵¹ The Canadian Office of the Privacy Commissioner has observed that:⁵²

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.

- 11.51 The potential for public visual surveillance to be overly broad or intrusive has led us to the view that specific guidance is needed on its use in a law enforcement context.

Social media monitoring

- 11.52 By “social media monitoring”, we refer to enforcement officers accessing social media to obtain information about individuals or classes of individuals. The term “social media” captures internet-based communication platforms that enable users to share information (including messages, videos, pictures and any other content).⁵³ Common examples include Facebook, Twitter and Instagram. However, this definition would also extend to media such as web forums and blogs, which allow people to post comments and interact with others.

- 11.53 Broadly speaking, there are two ways we are aware of in which social media monitoring could be used for law enforcement purposes. First, enforcement officers may conduct targeted searches to investigate a specific person or group. For example, an enforcement officer may look up a person’s Facebook profile to see whether they are “friends” with any known or suspected members of a criminal group or whether they have made any public posts indicating they are engaging in criminal activity.

- 11.54 Second, there are commercially-available algorithms that scan publicly available social media information to identify people or areas of possible concern (sometimes referred to as “data-mining”). These tools send out alerts when certain words or phrases are used in social media posts within a specific geographical area.⁵⁴ This functionality could be used, for example, to detect posts relating to drugs, gang activity or firearms. That information has the potential to assist in predicting or detecting crime, prompting preventative action or further investigation. Some algorithms used by overseas enforcement agencies assign “threat ratings” to individuals based on social media posts and other information available to those agencies.⁵⁵

- 11.55 Our discussion here relates to the passive monitoring of social media by enforcement agencies. A related issue is the active participation by enforcement officers in social media channels.

51 See paragraphs [11.21]–[11.22].

52 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).

53 Dictionary definitions include: “forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)” (*Merriam-Webster* “Social Media” < www.merriam-webster.com >) and “Websites and applications that enable users to create and share content or to participate in social networking” (*Oxford English Dictionary* “Social media” < <https://en.oxforddictionaries.com> >).

54 LexisNexis *One Step Ahead: How Social Media is Changing the Face of Investigations* (2013) at 5.

55 The “Beware” product is one example reportedly used by some police forces in the United States: see Conor Friedersdorf “A Police Department’s Secret Formula for Judging Danger” *The Atlantic* (online ed, Massachusetts, 13 January 2016).

This does not raise concerns where enforcement agencies have their own social media profiles, provided the identity of the agency is clear to the people that choose to interact with them. However, privacy issues may well arise where enforcement officers use fake profiles in order to befriend or interact with people through social media channels. This type of activity would be covered by the policy statement we recommend should be required for covert operations.⁵⁶

Why social media monitoring should be subject to policy statements

- 11.56 Social media is now a widely used form of interaction. Many social media platforms allow users to make content “private” so that it can only be seen by “friends” or “followers” approved by the user. Other social media content is “public”, meaning that it can be accessed by anyone. Enforcement agencies may view public content without needing to obtain any statutory authorisation. In many cases, this will be unobjectionable, since the user has chosen to make the information public. It can be compared to an enforcement officer walking down a street and hearing a conversation, or reading a “letter to the editor” in a newspaper.
- 11.57 Social media monitoring has the potential to be a valuable tool for law enforcement when it is used in a sufficiently targeted way. It could alert Police to immediate threats to public safety – for instance, if a person brags about a terrorist plot through social media channels. However, it also carries risks that do not arise—or at least not to the same extent—in respect of more traditional forms of public communications.
- 11.58 First, if social media monitoring becomes widely used by enforcement agencies, it has the potential to undermine the right to freedom of expression⁵⁷ and other associated rights.⁵⁸ It may discourage the public from engaging in debate and presenting opinions without fear of government interference. This is particularly likely if enforcement agencies use social media to monitor legitimate activity such as peaceful protest. For example, in the United States civil liberties groups criticised the Department of Homeland Security for reportedly monitoring social media information (including location data) relating to the Black Lives Matter campaign. The campaign was associated with widespread protests that followed the acquittal of police officer George Zimmerman on charges relating to the fatal shooting of Trayvon Martin.⁵⁹ There may be understandable reasons for such monitoring: for instance, there may be concerns that a peaceful protest could turn violent. However, the benefits of enforcement agencies having advance warning of threats must be weighed against the constitutional concerns that arise if people feel they may be targeted for expressing support for a cause or associating with a group.
- 11.59 Second, the use of social media monitoring as a predictive tool may raise concerns about discrimination against certain ethnic or religious groups. Say, for instance, that an algorithm is used to scan social media for terms that might be used by terrorists associated with the so-called Islamic State of Iraq and the Levant (ISIS). Those same terms may be used by Muslims in the legitimate expression of their religious beliefs. This may result in Muslims being subject to increased monitoring and investigation to confirm whether they are a threat or not. In turn, this may raise questions of discrimination on the grounds of religious beliefs and may discourage

56 Chapter 15 at paragraphs [15.125]–[15.128].

57 New Zealand Bill of Rights Act 1990, s 14: “Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form”.

58 These include the right to freedom of thought, conscience and religion (including the right to adopt and hold opinions without interference) (New Zealand Bill of Rights Act 1990, s 13), the right to manifest religion and belief in public or private (s 15) and the right to freedom of association (s 17).

59 The Intercept “Exclusive: feds regularly monitored Black Lives Matter since Ferguson” (25 July 2015) <<https://theintercept.com>>; Nusrat Choudhury “The Government Is Watching #BlackLivesMatter, And It’s Not Okay” (American Civil Liberties Union, 4 August 2015) <www.aclu.org>.

Muslims from exercising their rights to freedom of expression and freedom to manifest their religion in public.

- 11.60 Third, social media monitoring carries an increased risk that enforcement agencies may take action on the basis of inaccurate or misleading information. Statements made on the Internet are often exaggerated or intended to provoke a reaction without necessarily being a true reflection of the author's views. For example, the practice known as "trolling", which is common on social media platforms, involves deliberately starting arguments or posting inflammatory comments to provoke response. In other cases, slang terms may suggest meanings that are unintended. In 2012, two young British tourists were prevented from entering the United States under suspicion of terrorism after Tweeting that they planned to "destroy America" – a term they said was slang for partying.⁶⁰
- 11.61 Groups may also deliberately spread misinformation on social media as a means of evading government scrutiny. During the Standing Rock protests against the Dakota Access Pipeline in the United States, over a million people across the world "checked in" to Standing Rock on Facebook in an attempt to thwart rumoured attempts by Police to identify and surveil protesters.⁶¹ While Police denied they had been monitoring Facebook check-ins, the case demonstrates that social media information can be unreliable.
- 11.62 Finally, privacy issues may arise even though the information being monitored might be "publicly available". Privacy settings on social media platforms are often not well understood, and the automatic settings are subject to change. It may not be obvious to a user whether information they share on social media is "public" or not. Compared to other kinds of interactions in public places or forums, the line between what is public and what is private may be more difficult to draw. In addition, a person posting on social media may expect casual observation by peers but not intensive scrutiny by the State. Tools that collate and analyse significant amounts of information about individuals—for example, by combining their social media posts, location check-ins and the people and groups they associate with to assign "risk profiles" or predict offending—have the potential to intrude on reasonable expectations of privacy.⁶²
- 11.63 Because of these concerns, we consider it is important that enforcement agencies using social media monitoring exercise caution in deciding when it is appropriate to access information, what information is accessed and how it is stored and used. Given the complexity of the issues involved and the wide variety of potential uses of social media monitoring, consistent and context-specific guidance for enforcement officers is desirable. Furthermore, the transparency provided by policy statements is particularly important in light of the high rates of social media use and the public interest in ensuring that rights such as freedom of expression are not undermined.

Directed surveillance

- 11.64 By "directed surveillance", we mean observation or monitoring of an individual's movements or activities in circumstances not requiring a surveillance warrant. This would include activity by enforcement officers such as "stake-outs" of a person's house or following a suspect in a car. This category of public surveillance is, at this point in time, primarily aimed at observation carried out by enforcement officers in person (as opposed to using visual surveillance or other

60 Huffington Post "Leigh Van Bryan And Emily Bunting Banned From Entering US After Twitter Joke About 'Destroying America'" (30 January 2012) < www.huffingtonpost.co.uk > ; BBC News "Caution on Twitter urged as tourists barred from US" (8 March 2012) < www.bbc.com > .

61 Sam Levin and Nicky Woolf "A million people 'check in' at Standing Rock on Facebook to support Dakota pipeline protesters" *The Guardian* (online ed, San Francisco, 1 November 2016). A person would ordinarily "check in" to a location to indicate they are physically present there.

62 See paragraph [11.20].

technology). However, we have not limited our proposed definition in this way, as we wish to avoid categories of unregulated conduct that may develop as technology evolves. If technology can be used to monitor individuals and is not regulated by the surveillance warrant regime, it should be included in the policy statement.

- 11.65 For the sake of clarity, we note that policy statements would only need to address activities that any agency may wish to carry out. If a new technology could, in theory, allow directed surveillance but an agency does not intend to use it (either for practical reasons or because it is unlawful), it would not need to be covered by the policy statement.
- 11.66 We note there may be some overlap between directed surveillance and the other two types of public surveillance discussed above. Either visual surveillance or social media monitoring could be used in some cases to track the movements or activities of a particular individual. Provided that all of the relevant activities are covered by at least one policy statement, that would be sufficient.

Why directed surveillance should be subject to policy statements

- 11.67 Directed surveillance, at a basic level, forms part of the everyday activities of enforcement agencies. It is a core policing activity. Like public visual surveillance, it will often simply involve observing what any ordinary member of the public could observe. A police officer walking down the street may see a person acting suspiciously (for example, appearing to carry a knife) and observe them momentarily to ascertain whether any action is required; or a fisheries officer may observe people fishing to assess whether they are exceeding their catch. This type of activity is unlikely to raise public concern or require any detailed consideration by the enforcement officer.
- 11.68 In other cases, however, we consider that directed surveillance may intrude on expectations of privacy in the same way as public surveillance carried out using technology. That is particularly likely where the surveillance targets a particular individual over a prolonged period to obtain information about their movements or activities. For example, a sustained operation that involves enforcement officers monitoring a target round-the-clock to record their every move is comparable to the use of tracking technology. Although a different method is used, the level of intrusion on the person's privacy is no less. On the contrary, directed surveillance may be more intrusive to the extent that it provides more than just location information. For instance, it may disclose a high level of detail about a person's daily routine and who they associate with. In our view, individuals are entitled to expect that they will not be subject to intensive monitoring of this kind without justification.
- 11.69 We therefore consider that directed surveillance should be covered by a policy statement to ensure there are sufficient protections around the manner in which it is used. We note that such an approach is not without precedent. In the United Kingdom, legislation requires directed surveillance by enforcement agencies to be authorised by a senior person within the agency and covered by a code of practice issued by the Secretary of State.⁶³

Content of policy statements

- 11.70 As we have noted, policy statements would need to reflect both the principles we have recommended including in the Act and the principles in the Privacy Act (to the extent they are relevant). They would provide more specific guidance on how those principles apply to the activities covered by the statement, tailored to each enforcement agency's operating context.

⁶³ Regulation of Investigatory Powers Act 2000 (UK), ss 25(2), 26(2), 28 and 71.

11.71 We recommend that policy statements on public surveillance activities should include guidance on the following matters:

- *The purposes for which the activity may be carried out and the types of circumstances in which its use may or may not be appropriate.* By way of example:
 - It may be permissible to use CCTV to prevent or detect offending or security threats in high-risk areas, but combining it with facial recognition might only be appropriate for more limited purposes (for example, to locate people who are unlawfully at large, subject to electronic monitoring or suspected of an imprisonable offence).
 - The directed surveillance policy statement might indicate that monitoring an individual for more than a certain period of time is unlikely to be proportionate unless it is relevant to the investigation of an offence.
 - The use of social media monitoring might be limited to certain law enforcement purposes⁶⁴ to ensure it is not used to target legitimate activities such as peaceful protest.
- *When a specific warrant or order should be sought.* For example, using CCTV cameras to read private text messages or documents, or using x-ray to scan people or luggage, is likely to intrude on reasonable expectations of privacy. We would expect visual surveillance policies to indicate that a warrant should be applied for (or a statutory search power used) before undertaking such activity.⁶⁵
- *The manner in which the activity should be carried out in order to minimise the level of intrusion on privacy involved.* For example:
 - If social media monitoring is carried out using algorithms, guidance could be given on selecting appropriate search terms to help ensure the results are sufficiently targeted.
 - Where possible, enforcement agencies should make use of technology that allows them to only record information that is relevant for law enforcement purposes.⁶⁶
 - Policies should include guidance on the circumstances in which people should be notified that information about them is being collected and how that should occur.⁶⁷
- *Any internal approval, monitoring, reporting and record-keeping requirements that need to be complied with in particular situations.* For instance, directed surveillance continuing for more than a specified period of time might require sign-off at a particular level within the agency.
- *Requirements as to the use, storage and destruction of information obtained.* For example, Police guidance on CCTV provides that all recordings not required for evidential purposes must be erased within two months.⁶⁸

64 By way of comparison, s 92 of the Act provides that consent searches may be undertaken for the following purposes: to prevent the commission of an offence; to protect life or property, or to prevent injury or harm; to investigate whether an offence has been committed; or any purpose in respect of which the enforcement officer could exercise a power of search conferred by an enactment, if he or she held a particular belief or suspicion specified in the enactment.

65 See the discussion in paragraph [11.73] and onwards below.

66 For example, automatic number plate readers used by Police only capture images of cars that are of interest for law enforcement purposes, not all cars that drive past. See New Zealand Police “Technology helps get dangerous vehicles, high risk drivers and criminals off roads” (1 August 2014).

67 In accordance with principle 3 in s 6 of the Privacy Act 1993. For example, the Police CCTV guidance requires signs to be erected displaying the message “Police Crime Prevention Camera Area” (New Zealand Police *Crime Prevention Cameras (CCTV) in Public Places Policy* (May 2010)).

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

RECOMMENDATIONS

- R37 The Act should require policy statements to be issued in relation to:
- (a) the use of visual surveillance technology in circumstances not requiring a surveillance warrant (“public visual surveillance”);
 - (b) access to social media platforms to obtain information about individuals or classes of individuals (“social media monitoring”); and
 - (c) the observation or monitoring of an individual’s movements or activities in a manner not requiring a surveillance warrant (“directed surveillance”).
- R38 The policy statements covering public visual surveillance, social media monitoring and directed surveillance should include guidance on:
- (a) the purposes for which the activity may be carried out and the types of circumstances in which its use may or may not be appropriate;
 - (b) when a specific warrant or order should be sought;
 - (c) the manner in which the activity should be carried out in order to minimise the level of intrusion on privacy involved;
 - (d) any internal approval, monitoring, reporting and record-keeping requirements that need to be complied with; and
 - (e) requirements as to the use, storage and destruction of information obtained.

PUBLIC SURVEILLANCE NOT COVERED BY POLICY STATEMENTS

- 11.72 As we have explained, in our Issues Paper we discussed two different kinds of public surveillance:⁶⁹
- those that are already used but are not subject to specific regulation in a law enforcement context; and
 - those that are not in general use because there is significant doubt about whether they would amount to an unreasonable search under section 21 of NZBORA.
- 11.73 The discussion above has largely focused on the first category. We now turn to the second. Examples of activity in this second category include the use of detector dogs and chemical residue detectors to screen people or luggage for the presence of drugs or explosives in public areas. Certain activities that would be captured by the definition of public visual surveillance we have proposed are also likely to fall within this second category due to the level of intrusion they involve, such as the use of x-ray to screen people or luggage, or the use of cameras to read a person’s text messages on the screen of their phone.⁷⁰ Although these methods are used in public places, they allow enforcement agencies to see or obtain information about things that members of the public could not (for example, the concealed contents of a person’s pockets or luggage).

⁶⁹ Issues Paper, above n 33, at [3.104]–[3.129].

⁷⁰ Hence we have suggested above that the policy statement on public visual surveillance should indicate that a warrant should be sought before conducting these activities (see paragraph [11.71]).

- 11.74 The Supreme Court of Canada has held that the use of drug detection dogs in public places may intrude on reasonable expectations of privacy and amount to an unreasonable search.⁷¹ While there is not yet any New Zealand case law on the point, it is possible our courts would take a similar approach.
- 11.75 There are existing warrants, orders and powers in the Act that allow these types of methods to be used in particular circumstances. Dogs and equipment (such as chemical residue detectors or x-ray technology) may be used as an aid when executing a search warrant or exercising a warrantless power.⁷² Where the proposed use is for ongoing monitoring purposes rather than a discrete search, chemical residue detectors and x-ray would be covered by our proposed expanded definition of “visual surveillance technology”, so a surveillance warrant could, in theory, be sought. However, the conditions for issuing a search or surveillance warrant would need to be met,⁷³ and the warrant would need to be sufficiently targeted.⁷⁴
- 11.76 A declaratory order could also be issued if a judge considers the proposed use of the method is reasonable in the particular circumstances. This has already occurred on one occasion. Police obtained a declaratory order relating to the use of drug detection dogs at consenting domestic courier depots.⁷⁵
- 11.77 We do not recommend amending the Act to enable the wider use of these methods where an existing warrant or statutory power does not apply. Where that is the case, it is likely to be because the proposed use is insufficiently targeted (for example, if an agency wishes to carry out general screening of all people and luggage in a particular area, such as a train station) and/or insufficiently connected to the investigation of offending (for example, if the proposed use is for general crime detection purposes). In those circumstances the use of methods that intrude on reasonable expectations of privacy may be disproportionate to the public interest in law enforcement.
- 11.78 There may be some circumstances in which the use of intrusive methods for general screening purposes would be reasonable. However, we would be wary of specifically providing for them in the Act, as this may encourage greater use than is appropriate. In our view, it is preferable for any intended use of these methods to be assessed by a judge on a case-by-case basis through the declaratory order regime. As we explained in Chapter 6, declaratory orders can be issued in relation to activity for the purpose of preventing or detecting crime (rather than just investigating specific offences, like other warrants and orders).⁷⁶

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

72 Sections 110(e)–(e) and 125(f).

73 Sections 6 and 51. That is, there needs to be reasonable grounds to suspect a relevant offence has been committed and to believe the search or surveillance will obtain evidential material relating to the offence.

74 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [38], affirming *Auckland Medical Aid Trust v Taylor* [1975] 1 NZLR 728 (CA) at 733. There have been a number of instances where the courts have held that a warrant was overly broad and therefore invalid. See, for example, *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 (CA); *Calver v District Court at Palmerston North (No 1)* [2005] DCR 114, (2004) 21 CRNZ 371; and *F v R* [2015] NZCA 564 at [69] (where the Court held that the warrants in that case were unreasonably vague and general and therefore fundamentally defective).

75 New Zealand Police *Annual Report 2015/2016* at 152.

76 See paragraph [6.8].



Part 3

SEARCH

Chapter 12

Digital searches

INTRODUCTION

- 12.1 This chapter deals with the procedures that allow enforcement officers to search electronic devices, such as computers and mobile phones. These searches relate to stored data, rather than data that is in transit. If the data is in transit then enforcement officers must use surveillance powers as opposed to search powers. Surveillance powers are discussed in Chapters 7–10.
- 12.2 Under the Search and Surveillance Act 2012 (the Act), an electronic device is treated the same as any other receptacle, for example, a filing cabinet. Search warrants have always allowed an enforcement officer to search any filing cabinet at the place specified in a warrant if the filing cabinet may contain evidential material. No further authorisation is required. The Act adopts the same approach in relation to electronic devices.
- 12.3 As we explain in this chapter, we do not think that this approach is appropriate any longer. Changes in technology mean that electronic devices are now fundamentally different from ordinary receptacles. Electronic devices can store vast amounts of data, can generate data without the user’s involvement or even knowledge and can access data through the Internet that, technically, may be stored overseas. As recognised in recent case law, these developments have increased the privacy interest that attaches to electronic devices. They also raise complex issues of jurisdiction. We consider that dedicated rules should apply.
- 12.4 This chapter contains a series of interconnected recommendations that would significantly change how the Act deals with digital searches. Many of these recommendations reflect developments in recent case law. To explain these recommendations, it is necessary to explore complex legal matters and to use specialised terminology. We therefore begin by explaining the terminology we use and the way that we have structured the chapter. We also include a high-level summary of our recommendations to show how we see them fitting together.

TERMINOLOGY

Electronic device

- 12.5 We use the term “electronic device” in this chapter to describe any device that is capable of storing data. This includes computers, mobile phones, tablets, digital cameras, hard drives, USB sticks and memory cards. It should be noted that this is not the terminology that is used in the Act. Instead, the Act refers to “computer system or other data storage device”.¹ We prefer “electronic device” because it is shorter and seems more intuitive. We only use the phrases “computer system” and “data storage device” when we are expressly referring to provisions in the Act.

¹ See, for example, ss 110(h), 125(l) and 130 of the Search and Surveillance Act 2012.

Search of a device

- 12.6 This chapter focuses on searches *of the content* of electronic devices. However, during the execution of a search power, an enforcement officer may need to search *for* a device (for example, locate it within a house) or search *the actual* device (for example, to check that nothing is hidden in the battery compartment). In those circumstances, it is worth clarifying that where we use the phrase “search an electronic device”, we mean a search of the content of that device unless the context clearly indicates otherwise.

Digital search and Internet search

- 12.7 The most complex issues in this chapter arise from the fact that data may be accessible from an electronic device but not stored on that device. For example, a person can access their bank account statements from any electronic device using online banking, but the statements are not stored in those devices (unless they are downloaded). It is necessary to use the Internet to access them. As we explain in this chapter, there is uncertainty as to exactly how an enforcement officer should lawfully obtain access to this kind of online data when it is not publicly available.² That uncertainty is discussed at length in paragraphs [12.71]–[12.128]. Here we simply note that, when we use the phrase “digital search”, we are referring to any search of stored data, regardless of where it is stored. When we use the phrase “Internet search”, we are referring to a search of data that can only be accessed using the Internet.

STRUCTURE AND SUMMARY OF RECOMMENDATIONS

- 12.8 This chapter begins with an overview of the digital search provisions in the Act. This explains how warrantless powers and search warrants can be used by enforcement officers to lawfully search stored data. We then turn to consider whether the Act is keeping pace with developments in technology. We do so by examining recent New Zealand, Canadian and United States Supreme Court cases that have considered the changing nature of electronic devices.³ These cases recognise that electronic devices engage particularly high privacy interests and that therefore a search warrant should generally be required in order to search one.

The general warrant recommendations

- 12.9 In light of this case law, we explore whether the Act should be amended to place clearer warrant restrictions on searches of electronic devices. We conclude that it should and make five related recommendations. The first and second of these recommendations relate directly to the warrantless powers in the Act, which can only be exercised by New Zealand Police. We propose removing the automatic ability to search an electronic device during the lawful execution of a warrantless power. Instead, we recommend that, in the course of executing a warrantless power, a police officer should be able to seize and secure an electronic device. To search it, the officer should obtain a search warrant. Our second recommendation is that there should be one exception to this rule. A warrantless search of an electronic device should be permitted in urgent situations involving a risk to life or safety. These recommendations are discussed in paragraphs [12.32]–[12.43].
- 12.10 Our third and fourth recommendations give effect to our conclusion that a search warrant should only authorise a search of an electronic device if the device is expressly referred to in the

2 As we explain in paragraph [12.89], there is an international consensus that publicly available online data may be accessed by any enforcement officer regardless of where that data is stored.

3 This analysis begins at paragraph [12.26] with a discussion of *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745.

warrant. The degree of specificity required will depend on the nature of the warrant and the circumstances of the case.

- 12.11 Currently under the Act, a warrant can authorise the search of a “place, vehicle or other thing”.⁴ No changes to the Act are necessary if the warrant relates to a “thing”. If the “thing” is an electronic device, the Act already requires it to be described in sufficient detail to allow it to be readily identified. However, if the warrant relates to a “place or vehicle”, we recommend that the Act should require the warrant to expressly describe the electronic devices that may be searched at that location. This description needs to be as specific as the circumstances allow.
- 12.12 We further recommend that, since searches of electronic devices engage heightened privacy interests, the Act should be amended to highlight the option of an issuing officer including conditions in the warrant. This is discussed in paragraphs [12.63]–[12.66].

The jurisdiction recommendation

- 12.13 Having explained our general proposals in relation to search warrants and electronic devices, the chapter shifts to examine two issues that specifically relate to Internet searches:
- Are there issues of jurisdiction if the data that is searched using the Internet is actually stored on a server overseas?
 - How tightly constrained should Internet searches be?
- 12.14 We explore the issue of jurisdiction first at paragraphs [12.71]–[12.103]. We note that international law currently appears to prohibit an enforcement officer from directly accessing data through an electronic device in country A when that data is stored on a server in country B (a “cross-border Internet search”). This prohibition is subject to exceptions. Country B or the owner of the data may consent to the search. Alternatively, no consent is required if the data is publicly available. The international community is currently considering whether there should be additional exceptions to the prohibition. Those debates are taking place in the context of the Budapest Convention: a widely ratified international agreement dealing with cybercrime that New Zealand is not a party to.⁵
- 12.15 The significance of our jurisdiction discussion is two-fold. First, it leads us to recommend that the Government should consider whether New Zealand should accede to the Budapest Convention. Second, it partially explains why we think that additional constraints should be placed around Internet searches.

The Internet search recommendations

- 12.16 Having identified the risks associated with cross-border Internet searches, we conduct an assessment of the provisions governing Internet searches in the Act. We look at whether the provisions are sufficiently clear and whether they set appropriate parameters for Internet searches.
- 12.17 We start by looking at the definition of “computer system”.⁶ The Act clearly anticipates that a “computer system” includes data that is not stored on the computer itself but is stored within a

⁴ Search and Surveillance Act 2012, s 6.

⁵ Council of Europe Convention on Cybercrime ETS 185 (opened for signature 23 November 2001, entered into force 1 July 2004) [Budapest Convention].

⁶ Search and Surveillance Act 2012, s 3.

local area network.⁷ What is less clear is whether “computer system” includes any data that is only accessible from a device if it is connected to the Internet.

- 12.18 We explain that the answer to this question has a significant impact on how the remote access search provisions in the Act are understood.⁸ On the one hand, the remote access search provisions could be read as providing a specialised warrant regime for Internet searches. Alternatively, they could be read as simply enabling an enforcement agency to obtain a warrant to conduct an Internet search from its own office. We describe the latter scenario as “remote execution”.
- 12.19 We conclude that the Act does not clearly explain when an Internet search can be conducted or how extensive such a search can be. We therefore make five related recommendations. These recommendations are preliminary in nature because further consultation with technical experts is required to ensure that they are workable. First, we recommend that further consideration should be given to limiting the definition of “computer system” so that data on the system must be stored in New Zealand and must be accessible when the device is disconnected from the Internet. Second, we recommend repealing the remote access search provisions in the Act. We propose that, instead, further consideration should be given to amending the Act so that a search warrant could include “Internet access authorisation” and/or “remote execution authorisation”. This would allow an issuing officer to pre-authorise an Internet search and to set clear parameters for it. We also recommend that further consideration should be given to enacting a new warrantless Internet search power to reflect the fact that additional information may come to light during an Internet search and there may be no way to preserve relevant data pending a second warrant. These recommendations are set out in paragraphs [12.130]–[12.153].

The access information recommendations

- 12.20 The chapter ends by exploring whether the Act provides enforcement agencies with sufficient tools to obtain the passwords, decryption keys or other information that may be necessary to access an electronic device or an Internet site. Without that access information, any applicable warrant may be ineffective.
- 12.21 The main tool that is currently available to enforcement agencies is an offence provision in the Act. The Act creates a duty on every person who has knowledge of the access information for a device or an Internet site: that person must comply with a request by an enforcement officer executing a search power to provide that information.⁹ It is an offence to refuse without reasonable excuse.¹⁰ We make two recommendations in respect of these provisions.
- 12.22 First, we propose clarifying that the privilege against self-incrimination can only be claimed in order to justify a refusal in very limited circumstances. Second, we propose increasing the maximum penalty from three months’ to six months’ imprisonment. We acknowledge that this increase is unlikely to have a significant impact on compliance with the duty. That is because, unless the penalty is higher than any offence the person may be trying to conceal, there is no incentive to co-operate. However, since we elsewhere recommend that almost all searches of electronic devices should be conducted pursuant to a warrant, we think the increased penalty would better reflect the nature of any refusal. The person, in effect, would

7 A local area network is a computer network limited to a small geographical area such as an office building, university, or even a residential home.

8 The phrase “remote access search” is defined in s 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.

9 Search and Surveillance Act 2012, s 130.

10 Search and Surveillance Act 2012, s 178.

be frustrating the execution of a judicial order. These recommendations are discussed in paragraphs [12.169]–[12.172] and [12.177]–[12.179].

OVERVIEW OF THE PROVISIONS IN THE ACT

- 12.23 Under the Act, every person executing a search warrant or a warrantless search power is authorised to do certain things.¹¹ One of those things is that the person may use reasonable measures to access any “computer system or other data storage device” found (in whole or in part) at the relevant location¹² or in the possession of the person being searched.¹³ However, this is only permitted if the device may contain intangible material that is the subject of the search. This reflects the principle of functional equivalence. This principle was developed in the context of electronic commerce and is based on the idea that the laws designed for a paper-based environment can be applied by analogy in the digital environment.¹⁴ It treats an electronic device as if it is the same as any other receptacle found at a scene. These provisions allow an enforcement officer to search an electronic device on-site.
- 12.24 The Act also authorises an enforcement officer to remove an electronic device during a search and to arrange for it to be searched at an off-site location, where the officer is uncertain whether it contains evidential material and it is not reasonably practicable to determine that on-site.¹⁵ Further, the Act permits intangible material that is the subject of the search to be copied (by means of previewing, cloning, or other forensic methods) and searched off-site.¹⁶
- 12.25 As well as providing for on-site and off-site searches of electronic devices, the Act enables enforcement officers to apply for a search warrant to authorise a “remote access search”.¹⁷ A search warrant authorising remote access must relate to a “thing”, such as an Internet data storage facility, that is not situated at a physical location that can be entered and searched.¹⁸ Such a warrant authorises an officer to use reasonable measures to access the Internet data storage facility and to copy any online data that can lawfully be seized.¹⁹ These provisions were designed to enable enforcement officers to search online accounts, such as a Gmail account.²⁰

THE NATURE OF ELECTRONIC DEVICES

- 12.26 Since the Search and Surveillance Act came into force, the Supreme Courts in New Zealand,²¹ Canada²² and the United States²³ have all recognised that electronic devices engage unique privacy interests and that special rules for search and seizure apply. In *Dotcom v Attorney-General*, the New Zealand Supreme Court reviewed the rapidly growing jurisprudence on this topic and the majority concluded:²⁴

11 See, for example, s 110.

12 Section 110(h). “Computer system” is defined in s 3 of the Act. We discuss that definition below at [12.104]–[12.115].

13 Section 125(l).

14 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.12].

15 Section 112.

16 Sections 110(i) and 125(m).

17 Section 103(4)(k).

18 Sections 103(4)(k) and 103(6).

19 Section 111.

20 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.97].

21 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745.

22 *R v Vu* 2013 SCC 60, [2013] 3 SCR 657 and *R v Fearon* 2014 SCC 77, [2014] SCR 621.

23 *Riley v California* (2014) 134 S Ct 2473.

24 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [190]–[192].

[190] The overseas and New Zealand authorities accept the need, in relation to computers, for limits upon what is searched and seized in order to respect the right to be free from unreasonable search and seizure, and also for judicial oversight of decisions to issue search warrants.

[191] As *Vu*, *Fearon* and *Riley* illustrate searches of computers (including smart phones) raise special privacy concerns, because of the nature and extent of the information that they hold, and which searchers must examine, if a search is to be effective. This may include information that users believe has been deleted from their files or information which they may be unaware was ever created. The potential for invasion of privacy in searches of computers is high, particularly with searches of computers located in private homes, because information of a personal nature may be stored on them even if they are also used for business purposes. These are interests of the kind that s 21 of the Bill of Rights was intended to protect from unreasonable intrusion.

[192] Accordingly, 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 is believed is evidence of commission of an offence. For a warrant to include such authority there must have been sufficient sworn grounds in the application to support its issue in that form. This is consistent with the conclusion of the Canadian Supreme Court in *Vu* and the decision of the United States Supreme Court in *Riley*.

12.27 These cases mark a shift away from the principle of functional equivalence. As Cromwell J recently stated in giving the judgment for the Canadian Supreme Court in *R v Vu*:²⁵

[1] ... The traditional legal framework holds that once police obtain a warrant to search a place for certain things, they can look for those things anywhere in the place where they might reasonably be; the police do not require specific, prior authorization to search in receptacles such as cupboards and filing cabinets. The question before us is whether this framework is appropriate for computer searches; in short, should our law of search and seizure treat a computer as if it were a filing cabinet or a cupboard?

[2] In my view, it should not. Computers differ in important ways from the receptacles governed by the traditional framework and computer searches give rise to particular privacy concerns that are not sufficiently addressed by that approach.

12.28 The international jurisprudence recognises the following important ways in which electronic devices differ from other “receptacles”:²⁶

- They store immense amounts of information, some of which is likely to be of a highly private nature.
- They contain automatically generated information, which is often created without the user’s active involvement or knowledge. This includes versions of files, access details and browser histories.
- They retain files and data that the user may think have been deleted.
- They can continue to generate evidence even after they are seized.
- When connected to the Internet or a network, they act as portals to information that is not located, in any meaningful sense, at the same place as the device.

25 *R v Vu* 2013 SCC 60, [2013] 3 SCR 657 at [1] and [2].

26 *R v Vu* 2013 SCC 60, [2013] 3 SCR 657 at [41]–[44]; *R v Fearon* 2014 SCC 77, [2014] SCR 62 at [51] (majority) and at [128]–[133] (dissent); and *Riley v California* (2014) 134 S Ct 2473 at 19–22.

- 12.29 In relation to mobile phones and the Internet, the cases draw an analogy to a law enforcement officer finding a key in a suspect's pocket and arguing that it justifies entering and searching the suspect's home.²⁷
- 12.30 This jurisprudence is at odds with the provisions in the Act that govern the search of electronic devices. As indicated above, those provisions are based on the principle of functional equivalence. They reflect the following recommendation in the Law Commission's 2007 Report, *Search and Surveillance Powers*:²⁸
- Searches of computers should generally be regulated by the search and seizure regime that applies to tangible items (subject to necessary modifications) in preference to the creation of a different regime carrying more restrictive requirements.
- 12.31 That recommendation was made 10 years ago, in the same year that Apple released the first iPhone. By 2015, 70 per cent of all New Zealand adults owned or had access to a smartphone, and 91 per cent of those used their smartphone every day.²⁹ Changes to technology and the way in which people use it have prompted the courts to re-examine the question of whether special rules for digital searches are needed. It is important that the legislation reflects those developments.

A WARRANT REQUIREMENT

- 12.32 Sections 110(h) and 125(l) of the Act provide enforcement officers with an automatic ability to search electronic devices that are seized under a warrantless search power. By way of example, constables have a warrantless power to enter and search a place under the Act if the search is necessary to prevent the destruction of evidential material relating to serious offending.³⁰ If this warrantless power is exercised and an electronic device is seized (to prevent someone from destroying evidential material on the device), section 110(h) gives Police an immediate ability to search the contents of the electronic device. There is no need to obtain a search warrant first.
- 12.33 In our Issues Paper, we asked whether all searches of electronic devices should be conducted pursuant to a warrant. We also asked whether there should be an exception in urgent situations and/or a power to seize the device while a warrant is obtained.³¹ As we discussed in Chapter 4, the courts have frequently recognised the importance of having an independent and impartial person consider the justification for an intrusion on privacy *before* it occurs.³² We agree with that view. That is why we have recommended amending the Act to include the principle that a warrant or order should be obtained in preference to exercising a warrantless power.³³
- 12.34 Further, as we explained at the outset of this chapter, the Supreme Courts in New Zealand,³⁴ Canada³⁵ and the United States³⁶ have all recognised that there are special privacy concerns associated with electronic devices, given their ability to store significant amounts of information

27 *R v Fearon* 2014 SCC 77, [2014] SCR 621 at [132]; and *Riley v California* (2014) 134 S Ct 2473 at 21.

28 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) recommendation 7.1 and the discussion of the principle of functional equivalence at [7.11]–[7.20].

29 Research New Zealand *A Report on a Survey of New Zealanders' Use of Smartphones and other Mobile Communication Devices* (2015) at 3 and 9.

30 Search and Surveillance Act 2012, s 15.

31 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) question 33 [Issues Paper].

32 See, for example, *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 at [270].

33 Chapter 4 at paragraphs [4.28]–[4.43].

34 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745.

35 *R v Vu* 2013 SCC 60, [2013] 3 SCR 657 and *R v Fearon* 2014 SCC 77, [2014] SCR 621.

36 *Riley v California* (2014) 134 S Ct 2473. In *Riley*, the United States Supreme Court unanimously 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 serious injury), a search of a cell phone must always be done pursuant to a warrant.

of a personal nature.³⁷ There has also been a spate of recent cases in the Court of Appeal that recognise the high privacy interest attaching to electronic devices.³⁸

- 12.35 At present, it is unclear from the case law whether the powers in sections 110(h) and 125(l) are already constrained by the warrant preference approach. In other words, it is not clear whether a search of an electronic device (obtained in the course of exercising a warrantless power) would be unreasonable in terms of section 21 of the New Zealand Bill of Rights Act 1990 if a warrant could have been obtained in the circumstances. However, in *S v R* the Court of Appeal observed that:³⁹

It is a well-established principle that not all lawful searches are reasonable. In some circumstances, such as when there is no pressing need to carry out a search, the lawful exercise of a warrantless search power may still be unreasonable in terms of s 21 of [the New Zealand Bill of Rights Act 1990]. While most of the cases in this area are concerned with warrantless searches under the Misuse of Drugs Act 1975, we are persuaded that these principles have some application to the search of a digital device found on a person at arrest.

- 12.36 In light of the case law and the frequency with which this issue is likely to arise, we consider the position should be clarified in the Act.

Submissions

- 12.37 Enforcement agencies opposed any statutory warrant requirement. They noted that the current regime provides flexibility and means that evidence is not lost due to the inevitable delays that would result if a search warrant were required in all cases. As a practical illustration, Police advised that it is possible for electronic devices to be remotely wiped before investigators can search them. For instance, a person may configure their device to automatically wipe its contents if it remains stationary for a certain period of time. Alternatively, they could manually remove incriminating content by remotely accessing data stored on the device and data stored online that is accessible from the device. Enforcement agencies also emphasised that there is a wide range of electronic devices, and not all will hold or record extensive personal information.
- 12.38 Just over half of the submissions we received that addressed this point supported the introduction of a statutory warrant requirement. These submitters emphasised the prevalence of smartphones and other devices containing highly personal information. Most also supported the introduction of a power to seize a device and hold it while a warrant is applied for. They agreed this would align with section 117 of the Act (which allows for the preservation of a scene pending a warrant) and commented that it would focus the seizing officer's mind on whether there is true potential evidential value in the particular device.

Our view

- 12.39 We acknowledge that not all electronic devices contain highly personal information. However, the vast majority do – including the increasingly ubiquitous smartphone. We consider there is a need for an independent issuing officer to authorise the proposed search and to check that it

37 The Supreme Court in the United Kingdom and the High Court in Australia do not appear to have addressed these issues. We note, however, that the Law Commission of England and Wales has just begun a review of the law governing search warrants (see < www.lawcom.gov.uk/project/search-warrants/ >). We also note that the Supreme Court of Queensland has recently discussed the issue of warrantless searches of mobile phones in *R v N* [2015] QSC 91 at [57]–[63]. The Court discussed *Riley v California* (2014) 134 S Ct 2473 and observed that the decision reflects the current position in Queensland.

38 *M v R* [2017] NZCA 56; *S v R* [2016] NZCA 641; *Asgedom v R* [2016] NZCA 334; *S v R* [2016] NZCA 448; *M v R* [2015] NZCA 101; *Hoete v R* [2013] NZCA 432, (2013) 26 CRNZ 429. See also *Puna v R* [2016] NZCA 455 (which does not address these issues but does involve the warrantless search of a mobile phone) and *Lucas v R* [2015] NZHC 1944 (which was decided in the High Court).

39 *S v R* [2016] NZCA 641 at [38]. The Court found that there was a “pressing need” to search the appellant’s cell phone as there was a risk that evidence, in the form of photographs taken with the phone, could be destroyed. The clear implication of this finding is that if there had been no such risk, a search warrant should have been obtained.

is appropriately tailored to the circumstances of the individual case.⁴⁰ We therefore recommend that, as a general rule, an electronic device may be seized and secured during the execution of a warrantless power (if the device is relevant to the power being exercised) but its contents may not be searched without the enforcement officer first obtaining a warrant authorising that search. The device must be returned if a warrant is not obtained within a reasonable timeframe.⁴¹

- 12.40 We are of the view that the introduction of a statutory power to seize and secure a device will negate the concerns raised regarding the destruction of evidence. Most of those concerns can be addressed by securing the device. This could be done by putting the device into flight mode,⁴² turning the device off, placing the device in a faraday bag⁴³ and/or by storing it in a location that has no Internet connection. We understand this is already routine law enforcement practice in order to preserve the integrity of electronic evidence.
- 12.41 We acknowledge that this approach does not address the issue of online data being remotely destroyed before law enforcement agencies can view it. However, as we explain further below, we are not convinced that such data forms part of the “computer system” an enforcement officer is authorised to search. Therefore its destruction is no different from a person destroying physical evidence before a warrant can be obtained to search for it.
- 12.42 However, we do think that in some urgent circumstances a warrantless search of an electronic device should be able to occur. This may require data to be accessed via the Internet. We discuss Internet searches later in this chapter. Here it is sufficient to say that we consider these circumstances are likely to be exceptional. We suggest that an exception based on urgency could be framed in a similar manner to section 14 of the Act, which enables warrantless entry to prevent an offence or respond to a risk to life or safety. That section only applies in circumstances where:
- an offence is being committed, or is about to be committed, that would be likely to cause injury to any person, or serious damage to, or serious loss of, any property; or
 - there is risk to the life or safety of any person that requires an emergency response.
- 12.43 Finally, we note that our recommendations concerning warrantless powers in this chapter only relate to the police powers in Part 2 of the Act. As we foreshadowed in Chapter 2, further work should be undertaken in respect of the warrantless powers listed in the Act’s Schedule, which apply to other enforcement agencies, to determine what the impact of these recommendations might be.⁴⁴

40 Through application of the minimal intrusion principle and potentially imposing conditions as discussed below at paragraphs [12.63]–[12.66].

41 The length of an appropriate timeframe should be the subject of specific consultation with enforcement agencies.

42 Flight mode is a setting on a mobile phone or other electronic device 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 prohibited.

43 A faraday bag is specifically designed to assist in securing electronic devices. The bag prevents the device from connecting to the Internet or cellular networks.

44 Chapter 2 at paragraph [2.84].

RECOMMENDATIONS

- R39 Sections 110(h) and 125(l) of the Act (which outline the powers of search) should be amended to remove the ability for a person executing a warrantless search power under Part 2 of the Act to automatically search an electronic device if the device may contain intangible material that is the subject of the search. This should be replaced by a power to seize and secure such a device, pending determination of an application for a search warrant authorising a search of the contents of the device.
- R40 A provision should be inserted into the Act to enable an electronic device that is obtained during the execution of a warrantless search power under Part 2 of the Act to be searched without a warrant in urgent circumstances. The circumstances should align with those described in section 14(2) of the Act.

THE CONTENT OF THE WARRANT

The degree of specificity

- 12.44 Related to the issue of when a warrant is required is the question of how specific the warrant needs to be. A search warrant can be issued in respect of a “place, vehicle, or other thing”.⁴⁵ If an electronic device is the “thing” that a warrant relates to, it must be described in sufficient detail to allow it to be readily identified. This is how a warrant application would be framed if an electronic device was seized and secured by Police during the execution of a warrantless power under the Act. The device would be easy to identify in the application as it would already be in police custody. However, if an electronic device may contain intangible material that is the subject of a warrant issued in respect of a place or vehicle, would it be sufficient for the device to be found at the location named in the warrant or does the warrant need to expressly refer to the device? If the latter approach is taken, does the particular device need to be identified or is it sufficient for it to be covered by a broad description, for instance, of the type of devices that may be present?
- 12.45 These questions arise as a result of the Supreme Court’s analysis in *Dotcom v Attorney-General*.⁴⁶ The Court was asked to determine whether search warrants issued under the Mutual Assistance in Criminal Matters Act 1992 and the Summary Proceedings Act 1957 were overly broad and, in effect, amounted to general warrants “against which the law has long set its face”.⁴⁷
- 12.46 Significantly, the search warrants identified the evidence sought as including “all digital devices, including electronic devices capable of storing and/or processing data in digital form”.⁴⁸ The warrants then provided an inclusive list of the types of devices that the applicant expected to find. The appellants claimed that this description was one of several overly broad aspects of the warrants.
- 12.47 In traversing the underlying principles relating to general warrants, the majority decision in *Dotcom* cited the Court of Appeal’s decision of *Tranz Rail Ltd v Wellington District Court* with approval.⁴⁹ In that case the Court of Appeal described a general warrant as “a warrant which

45 Search and Surveillance Act 2012, s 6.

46 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745.

47 At [69].

48 At [87].

49 At [99] and [112]–[113].

does not describe the parameters of the warrant, either as to subject-matter or location, with enough specificity”.⁵⁰ As we noted in Chapter 4, the Court further observed:⁵¹

Both the person executing the warrant, and those whose premises are the subject of the search, need to know with the same reasonable specificity, the metes and bounds of the Judge’s authority evidenced by the warrant.

- 12.48 The majority in *Dotcom* also reviewed the relevant authorities in New Zealand, Canada and the United States, including *R v Vu*,⁵² *R v Fearon*⁵³ and *Riley v California*.⁵⁴ As *Riley* and *Fearon* were both cases involving warrantless search powers, the decision in *Vu* is the most relevant.
- 12.49 In *Vu*, the Canadian Supreme Court unanimously decided that, before any “computer” can be searched, a judge asked to issue a warrant must specifically address whether there are reasonable grounds to believe that the computer will contain relevant material and whether the particular privacy interests that may be affected by the computer search are outweighed by State law enforcement interests.⁵⁵ The Court treated a computer as “a separate place of search necessitating distinct prior authorisation”.⁵⁶ It considered that the right to be free from unreasonable search and seizure requires such prior consideration and specific authorisation.⁵⁷
- 12.50 The majority in *Dotcom* adopted the reasoning in *Vu* but observed that the factual scenario was significantly different. The search warrant in *Vu* did not specifically refer to any computer or electronic device whereas the warrants in *Dotcom* did. The majority did not express concern about the broad description of the devices in the warrants, given the nature of the alleged offending.⁵⁸ It was sufficient that the issuing officer had been made aware that the warrants would relate to electronic devices and had been provided with an explanation of why a search of such devices was necessary. On this point, the majority concluded:⁵⁹
- ... 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 is believed is evidence of commission of an offence.
- 12.51 The authors of *Adams on Criminal Law – Rights and Powers* have questioned whether this degree of specificity is required for a warrant issued under the Search and Surveillance Act, given that the warrants in *Dotcom* were issued before the Act came into force. The authors explain:⁶⁰

This decision related to a search under the now repealed provisions of the Summary Proceedings Act 1957. It may be doubted whether it applies to searches conducted under the Search and Surveillance Act 2012, since s 110 allows access to a computer system in relation to any lawful search to which the Act applies, whether or not it is specifically authorised by the warrant or warrantless power. In *Hager v Attorney-General* [2015] NZHC 3268 at [138], the Court assumed, without specifically considering the point, that it does apply.

50 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [38].

51 At [41].

52 *R v Vu* 2013 SCC 60, [2013] 3 SCR 657.

53 *R v Fearon* 2014 SCC 77, [2014] SCR 621.

54 *Riley v California* (2014) 134 S Ct 2473.

55 *R v Vu* 2013 SCC 60, [2013] 3 SCR 657 at [47]–[49].

56 At [54].

57 At [50]–[51].

58 The appellants in *Dotcom* had been charged in the United States with racketeering, money laundering and copyright infringement. Some of the charges had an express digital element, namely: criminal copyright infringement “by distributing a work on a computer network” and “by electronic means”.

59 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [192].

60 Simon France (ed) *Adams on Criminal Law – Rights and Powers* (online looseleaf ed, Thomson Reuters) at [SS110.12].

- 12.52 We do not think that the power in section 110(h) of the Act should be read as negating the requirement that a warrant must be as specific as the circumstances allow.⁶¹ The need for warrants to be as specific as reasonably possible is an important component of the minimal intrusion principle that we have recommended in Chapter 4, which applies to both digital and non-digital searches.
- 12.53 We therefore consider that, if evidential material may be found in an electronic device, that fact should be brought to the attention of an issuing officer and should be referred to in the content of any warrant. The issuing officer needs to be in a position to turn their mind to the special concerns that arise in searches of this nature. In some circumstances, like in *Dotcom*, the description of the devices and what data may be searched may need to be fairly general. It may not be possible for enforcement agencies to know in advance exactly what devices may be at a scene and what data may be stored on them. In other circumstances, like those in *A Firm of Solicitors v District Court at Auckland*,⁶² a similarly broad description may be inappropriate.
- 12.54 To explain how we envisage this requirement working in practice, it is worth considering two examples: if a business is under investigation for fraud, it may be sufficient for a warrant in respect of its headquarters to refer to “all desktop computers, laptops and tablets that there are reasonable grounds to believe are associated with the business and contain evidential material”. On the other hand, if a person is suspected of sending abusive text messages and lives in a flatting situation, the warrant would need to contain greater detail. For instance, “any mobile phone located within the flat that is associated with person x and/or the telephone number 1234567”. Much will depend on the factual scenario and the alleged offending in each case. At the very least, however, the issuing officer needs to know that a search of an electronic device is likely to be required.
- 12.55 If an electronic device is found during the execution of a search warrant but is not identified (either specifically or under a broader description) in the warrant itself, we do not consider that section 110(h) of the Act should continue to permit the device to be searched. Searches should not exceed the authority conferred by the warrant.⁶³ As explained in paragraphs [12.23]–[12.31], section 110(h) is based on the outdated idea that an electronic device is the functional equivalent of a filing cabinet. We consider that an electronic device is more akin to being a different “place”. We envisage, however, that warrant applications would regularly contain references to electronic devices, as it is common for them to contain evidential material. What matters is that enforcement officers and issuing officers consider the prospects of a digital search in advance.

Other mechanisms to promote targeted searching

- 12.56 In our Issues Paper we asked whether the Act should be amended to limit the amount of irrelevant material that is seen during a search of an electronic device. We discussed three options:

61 This issue does not arise under s 125(l) of the Act, as that provision deals with searches of the person, which are always conducted pursuant to warrantless powers.

62 In *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 (CA) the search warrant included generic items such as “[e]lectronic media (including floppy discs, hard drives, hard copy, CDs)” and “[h]and held computers, or other electronic storage devices”. The Court of Appeal held that the warrants were “clearly too broad” (at [79]), particularly since there were no additional qualifiers as to the type of data that could be searched. See also *Bielawski v Police* [2014] NZHC 2653, *Calver v District Court at Palmerston North* (No 1) (2004) 21 CRNZ 371 (HC), *Gill v Attorney-General* [2010] NZCA 468, [2011] 1 NZLR 433 and the discussion in Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.53]–[7.56].

63 We note, however, that a search of a device that is not described in the warrant will not necessarily be unreasonable in terms of s 21 of the New Zealand Bill of Rights Act 1990. As we explained in Chapter 3 at paragraph [3.22], the reasonableness inquiry is a highly fact-dependent exercise that involves balancing all the relevant values and public interests involved.

- a requirement that an issuing officer must consider the appropriate search process and whether to impose conditions on any warrant that relates to an electronic device;⁶⁴
 - a requirement that any person who searches an electronic device must produce a written record of their search procedure;⁶⁵
 - a duty on an enforcement officer to take all reasonable steps to minimise access to irrelevant material during any search of an electronic device.⁶⁶
- 12.57 We have already recommended in Chapter 4 that the Act should be amended to include a principle that the powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any persons likely to be affected. Therefore the question to be answered here is whether any further amendments are necessary to reflect the privacy interests associated with searches of this nature.
- 12.58 All 12 of the submissions and comments we received on this question agreed with the general proposition that enforcement officers searching electronic devices may view more material than is necessary for the purpose of the search. However, most submitters stated that this is an inevitable feature of digital searches.
- 12.59 Enforcement agencies explained that the material that is viewed is necessary to allow the person searching the device to navigate the system, establish what is present and make determinations as to what is relevant. It is inevitable that some irrelevant material will be seen, as evidential material can be embedded in other material or held in apparently innocuous folders. Forensic screening tools (such as keyword searching) are used to filter out irrelevant material but this may require a process of trial and error. For example, foreign language content, images and encrypted data may not be amenable to keyword searching. Further, warrants are often issued early on in investigations and it may not be practical at that stage to be precise about what could amount to evidential material.
- 12.60 For these practical reasons, we have concluded that search warrants that relate to electronic devices cannot be too prescriptive in terms of the search process that they authorise. There must be sufficient flexibility to allow the search process to respond to the challenges posed by particular devices as they arise. As noted by the New Zealand Law Society, it is impossible to eliminate the risk of seeing irrelevant material without unacceptably curtailing the legitimate exercise of search powers.
- 12.61 Nevertheless, we consider that the owner of an electronic device still has a reasonable expectation of privacy in that device after it is seized.⁶⁷ This means that the search of the device must be conducted in a reasonable and therefore targeted manner. The device is not an “indivisible object of search” that, like pieces of physical evidence, can be tested and inspected in whatever ways an enforcement agency deems necessary.⁶⁸ This conclusion is supported by the fact that the “plain view rule”⁶⁹ applies to searches of electronic devices.
- 12.62 As discussed in our Issues Paper, the plain view rule allows for evidence of offending to be seized if that evidence is discovered incidentally during the course of a lawful search related to a different offence.⁷⁰ Some commentators have called for the rule to be abandoned in relation

64 Issues Paper, above n 31, at [6.45].

65 At [6.42].

66 At [6.52].

67 See *R v Jones* 2011 ONCA 632 at [45]; and, more generally, *R v Vu* 2013 SCC 60, [2013] 3 SCR 657 and *R v Morelli* [2010] 1 SCR 253.

68 *R v Jones* 2011 ONCA 632 at [45]–[46].

69 See s 123 of the Search and Surveillance Act 2012.

70 Issues Paper, above n 31, at [6.27]–[6.28].

to digital searches because of the amount of material that can incidentally be seen.⁷¹ The only rational basis for retaining the rule is if digital searches are carried out under strict, planned and targeted parameters. We think that the rule should be retained, because without it, evidence of serious offending that is legitimately found during a targeted search could not be used in any prosecution. However, the Act needs to emphasise the need for targeted searches to ensure that the plain view rule does not encourage or permit fishing expeditions.

Conditions

- 12.63 Submitters were divided as to the efficacy of requiring issuing officers to consider imposing conditions. Those in favour emphasised that conditions could usefully address the special privacy concerns associated with digital searches. Those against did not think it would be possible to impose workable, practical conditions and thought that issuing officers were unlikely to have the requisite expertise to impose appropriate conditions. One submitter observed that the field of digital forensic analysis is rapidly evolving and there is a real risk that issuing officers' knowledge of what is current best forensic practice would quickly become outdated.
- 12.64 Having reviewed the arguments on both sides, we are not convinced that a requirement to impose conditions would be useful in every case. It seems to us that a certain degree of flexibility is needed when searching electronic devices, given that the searcher is unlikely to know in advance exactly where and in what format the targeted material is stored. There is a risk that investigations would be hindered through the routine imposition of unworkable or unduly prescriptive conditions.
- 12.65 We do think, however, that the Act should place more of an emphasis on the option of imposing conditions on digital searches. We envisage that applicants would be asked for their input on appropriate conditions and that issuing officers would be provided with sufficient information about developments in forensic practice to make informed decisions on the appropriate course of action.
- 12.66 This policy could be achieved by amending section 103(3)(b) of the Act. That section currently states that a search warrant can be subject to any conditions that the issuing officer considers reasonable and includes two examples. We recommend including a third example along the following lines: "any condition to minimise the level of intrusion on the privacy of any person likely to be affected during a search, including a search of a computer system or other data storage device". Framing the example in this way mirrors the corresponding principle that we recommended in Chapter 4. It also recognises that, whilst there may be a particular need for this type of condition in respect of digital searches, the need may also arise in respect of other searches.

Record-keeping

- 12.67 In our Issues Paper we suggested that a record-keeping requirement may promote greater accountability and transparency around the process of searching electronic devices. It could also have the related effect of reminding enforcement officers to focus on the question of whether they are conducting a targeted search. The opinion of submitters was divided.
- 12.68 Of particular note were the submissions from agencies that employ specialist digital forensic staff. Those agencies advised that these specialists are always mindful of the need to conduct targeted searches, for principled reasons and also as a result of time and resource constraints. They observed that specialists already make technical notes of the steps involved but argued that

⁷¹ See the discussion in Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.68]–[7.73] and in David Harvey *Internet.law.nz* (4th ed, LexisNexis, Wellington, 2016) at [8.286]–[8.333].

creating a more accessible detailed record in every case would be impractical. They suggested that such a requirement could significantly impede investigations given the large number of files that may need to be reviewed and the large number of keyword searches and other filters that may need to be used to find those files.

- 12.69 In light of those observations, we consider that a record-keeping requirement is not appropriate in cases where the search is conducted pursuant to a search warrant or in an urgent situation. If there is a warrant, there is scope for case-specific conditions to be put in place. If the situation is urgent and is premised on responding to an emergency rather than collecting evidence, a record-keeping requirement would be unduly onerous. We do, however, think that a record-keeping requirement should attach to warrantless Internet searches, as discussed at paragraph [12.152] below.

A statutory duty

- 12.70 We do not favour the option of imposing a statutory duty on enforcement officers to take all reasonable steps to avoid seeing irrelevant material when searching a device. Such a duty would likely be difficult to apply in practice, since enforcement officers will necessarily have to look at some irrelevant material in order to identify evidential material. We are of the view that the principle of minimising intrusion, which we have recommended in Chapter 4, achieves the same goal. The principle has the benefit of applying to all searches, not just digital searches. Further, it avoids the problem of being framed as a negative duty.

RECOMMENDATIONS

- R41 Section 103(4) (which explains what a search warrant must contain) should be amended to include a statement that every search warrant must contain, in reasonable detail, a description of any computer systems or other data storage devices that may be seized and searched.
- R42 Section 110(h) (which explains that a person exercising a search power may access a computer system or other data storage device) should be amended to permit access only where the device is described in the warrant and may contain intangible material that is the subject of the search.
- R43 Section 103(3)(b) (which states that a search warrant may be subject to conditions) should be amended to include a third example of the types of conditions that could be specified in a search warrant. The example should be framed along the following lines: “any condition to minimise the level of intrusion on the privacy of any person likely to be affected during a search, including a search of a computer system or other data storage device”.

ISSUES RAISED BY INTERNET SEARCHES

- 12.71 As explained in our introduction to this chapter, we consider that there are unique legal and policy issues associated with Internet searches. Given that enforcement officers are increasingly likely to need to search online data that is not publicly available, it is important to ensure that the statutory framework is robust.
- 12.72 The provisions in the Act that govern Internet searches are largely based on the recommendations made in the Law Commission’s 2007 Report. Since that Report, however, there has been an exponential growth in the use of cloud computing. As we discussed in Chapter 2, cloud computing is a method of storing and accessing data and programs using

remote servers hosted on the Internet rather than on a local server or electronic device.⁷² Data stored in the Cloud may therefore be distributed over different servers, providers, locations and often jurisdictions. The location of that data may also be constantly changing. In practical terms, this means that the location of much of the data stored “in the Cloud” may be unknowable.

- 12.73 The remote access search provisions in the Act enable the search of “a thing such as an Internet data storage facility that is not situated at a physical location”.⁷³ As we explain further at paragraphs [12.117]–[12.118] below, these provisions are a clear indication that Parliament intended the Act to enable searches of data that is stored in the Cloud in an unknowable location. What is not clear, however, is whether the remote access search provisions are the only provisions in the Act that enable an Internet search. As we discuss in paragraph [12.108], the definition of “computer system” in the Act is arguably broad enough to include any data that is accessible from a device using the Internet. A clear framework is critical because as soon as the door to the Internet is opened, the parameters of any search become blurred. Without appropriate constraints it would be very easy for enforcement officers to access data that is stored in a known or knowable overseas location. It is not clear whether Parliament intended the Act to apply to that type of data.
- 12.74 The Law Commission described remote access searching as “one of the most difficult areas” dealt with in its 2007 Report. At that time, the Commission noted the “inconclusive state of international law” and commented: “[i]t is possible that over time, sensible limits on cross-border searches will develop and that States may come to accept such searches as legitimate”.⁷⁴ Ten years later, it appears that States still have not reached the conclusion that this practice is legitimate, although the matter is currently the subject of widespread international attention.
- 12.75 We agree with those who submitted to us that the process of searching online data that is not publicly available will often raise international issues. Therefore, we consider that it is important in developing policy in this area to take into account the recent developments in international customary law and State practice.

Customary international law

- 12.76 Under customary international law and therefore New Zealand law,⁷⁵ no country can conduct an investigation in another country without prior authorisation. This is seen as an unlawful extension of the first country’s jurisdiction to enforce its laws.⁷⁶ Instead, the traditional solution for obtaining foreign evidence in criminal matters is State-to-State co-operation, usually in the form of mutual legal assistance agreements. This approach is designed to preserve international relations, and to promote the rule of law and safeguards that protect privacy.
- 12.77 There has been considerable debate as to whether this rule applies to law enforcement officers who obtain data from overseas via a cross-border Internet search. This is often described as a

⁷² Chapter 2 at paragraphs [2.66]–[2.67].

⁷³ Section 103(4)(k) of the Act.

⁷⁴ Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.116].

⁷⁵ Customary international law is part of New Zealand’s common law. See *Attorney-General v Zaoui* [2005] NZSC 38, [2006] 1 NZLR 289 at [24]; Campbell McLachlan *Foreign Relations Law* (Cambridge University Press, Cambridge, 2014) at [3.28]; Alberto Costi *International Law: Principles* (Reissue 2, LexisNexis, Wellington, 2016) at 128; Alice Osman “Demanding Attention: The Roles of Unincorporated International Instruments in Judicial Reasoning” (2014) 12 NZJPIIL 345 at 347; and Alan Bracegirdle “Domestic procedures for International Treaty Actions: The courts and unincorporated treaties in New Zealand” (2005) 20 Australian Parliamentary Review 54 at 59.

⁷⁶ A distinction is generally made between prescriptive jurisdiction (also known as legislative jurisdiction) and jurisdiction to enforce (also known as executive jurisdiction). The first relates to the power to make laws and decisions. The second relates to the power to enforce those laws and includes the power to investigate offending. It is relatively common for States to exert extraterritorial prescriptive jurisdiction (in accordance with certain accepted ‘heads’ of jurisdiction), whereas extraterritorial jurisdiction to enforce is generally prohibited unless the other State consents: see Campbell McLachlan *Foreign Relations Law* (Cambridge University Press, Cambridge, 2014) at [11.07]–[11.10]; Roger O’Keefe *International Criminal Law* (Oxford University Press, Oxford, 2015) at [1.6]–[1.13]; and Anna-Maria Osula “Transborder access and Territorial Sovereignty” (2015) 31 CLS Rev 719 at 721.

type of “trans-border access to data”. The reason for the debate is that the law enforcement officer can access this data without ever physically setting foot in the other country, so there is no overt affront to sovereignty. The debate has recently been summarised by Anna-Maria Osula as follows:⁷⁷

Despite there being views on transborder access that argue the activity to be generally in line with territorial sovereignty, neither States nor international organisations have univocally approved such access without any additional legal grounds such as the consent of the other State, nor is the legality of transborder access widely supported by scholars. In fact, according to a recent UN study, around two-thirds of countries in all regions of the world perceived foreign law enforcement’s access to other State’s computer systems or data as impermissible, even if it may occur in practice either with or without the knowledge of investigators.⁷⁸

12.78 Having reviewed the relevant literature and current State practice, Osula concludes:⁷⁹

... we have established that a State accessing data in a foreign jurisdiction could be considered an extra-territorial application of jurisdiction to enforce, and without the right deriving from an international treaty or the consent of the other State, could be considered a breach of territorial sovereignty.

State practice

12.79 To assess the possible risk to international relations posed by a cross-border Internet search of data that is not publicly available, it is necessary to look at how other countries are grappling with this issue. In that regard, the approach taken by the United States is significant, because the headquarters of many of the world’s largest multinational service providers are located there.⁸⁰ As such, much of the data that is likely to be of interest to New Zealand law enforcement officers is also likely to be stored there.

The United States

12.80 The United States appears to be acutely aware of the problems associated with trans-border access to data. The following developments are worth noting:

(a) In a 2009 manual on the search and seizure of electronic data, the Department of Justice provided the following advice to Federal Prosecutors:⁸¹

When agents learn before a search that some or all of the data is stored remotely outside of the United States, matters become more complicated. The United States may be required to take actions ranging from informal notice to a formal request for assistance to the country concerned. Further, some countries may object to attempts by U.S. law enforcement to access

77 Osula “Transborder access”, above n 76, at 725. See also B J Koops and M Goodwin *Cyberspace, the Cloud and Cross-Border Criminal Investigation* (Tilburg Institute for Law, Technology, and Society, The Netherlands, 2014) at 42; Stewart M Young “Comment: Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases” (2003) 10 Mich Telecomm Tech L Rev 139; Jack L Goldsmith “The Internet and the Legitimacy of Cross-border Searches” (2001) U Chi Legal F 103; Patricia L Bellia “Chasing Bits Across Borders” (2001) U Chi Legal F 35; Michael A Sussmann “The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium” (1999) 9 Duke J Comp & Int’L 451; Paul Hunton “Managing the Technical resource capability of Cybercrime Investigation: a UK Law Enforcement Perspective” (2012) 32(3) Public Money and Management 225.

78 United Nations Office on Drugs and Crime *Comprehensive Study on Cybercrime* (February 2013) at 220–223.

79 Osula “Transborder access”, above n 76, at 727.

80 In this Report, we use the term “service provider” to refer to private sector businesses that provide a service to customers. This includes telecommunications network operators, internet service providers, banks, electricity and gas suppliers and transport companies.

81 Orin S Kerr *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3rd ed, Office of Legal Education, Executive Office for United States Attorneys, 2009) at 85.

computers located within their borders.⁸² Although the search may seem domestic to a U.S. law enforcement officer executing the search in the United States pursuant to a valid warrant, other countries may view matters differently. Agents and prosecutors should contact the Office of International Affairs ... for assistance with these difficult questions.

- (b) As discussed in our Issues Paper, the high-profile September 2016 decision of *Microsoft Corporation v United States of America* was concerned with similar issues.⁸³ In that case, the Second Circuit Court of Appeals quashed a search warrant that purported to require Microsoft in the United States to produce the contents of a user's Outlook email account, which was stored on servers in Ireland.⁸⁴ Microsoft in the United States could access this data using its computer system, but the Court held that the warrant did not have extraterritorial application and so could not apply to data stored overseas.⁸⁵
- (c) In December 2016, the United States amended Rule 41 of the Federal Rules of Criminal Procedure. The amendment was controversial.⁸⁶ It allows a magistrate judge to issue a warrant to remotely search "a computer" located outside of the judge's district, if (1) the physical location of the information is "concealed through technological means" or (2) "a number of computers" (located in five or more districts) have been infected with malware, which allows the computers to be controlled as a group without the owners' knowledge. A third change requires the government to "make reasonable efforts" to notify the person whose electronically stored information has been remotely searched. The Department of Justice advised that such warrants would have "no extraterritorial effect".⁸⁷

The United Kingdom

- 12.81 It is not entirely clear whether direct trans-border access to data is lawful in the United Kingdom.⁸⁸ The primary power in the United Kingdom to conduct a search pursuant to a warrant for the purpose of a criminal investigation is contained in section 8 of the Police and Criminal Evidence Act 1984 (UK) (PACE). The legislation provides powers of both search and seizure. The preconditions for issuing a warrant under that section are similar to those in section 6 of the Search and Surveillance Act.
- 12.82 For the purposes of a warrant issued under section 8 of PACE, the material that is the subject of the warrant must be "on" the premises. In relation to searches for evidence in electronic

82 This comment may be linked to the high profile 2001 case of *United States v Gorshkov* 2001 WL 1024026 (W D Wash 2001). There, the Federal Bureau of Investigation (FBI) traced hackings of banks, internet service providers and other United States firms to suspects using data servers in Russia. After failing to get Russian assistance in monitoring the criminal activity, the FBI acted unilaterally and obtained a search warrant in the United States. The FBI used a keystroke recording program to gather user names and passwords that allowed access to the Russian servers and downloaded incriminating information. The Russian Government responded by laying criminal charges against the FBI investigators.

83 *Microsoft Corporation v United States of America* 829 F 3d 197 (2d Cir 2016) at 39.

84 Microsoft's headquarters are in the United States but its subsidiaries operate separate data centres. In this case the relevant data was stored in a data centre in Ireland. The case turned on the Court's interpretation of United States law, specifically whether the Stored Communications Act (US) empowers a United States magistrate judge to issue a search warrant with extraterritorial application. There was no consideration of Irish law.

85 After the decision in *Microsoft Corporation v United States of America* was delivered, the United States Department of Justice petitioned for rehearing. However, in January 2017, the Second Circuit Court of Appeals denied the rehearing by a 4-4 vote. See *Microsoft Corporation v United States* No 14-2985 (2d Cir 2017).

86 Susan Hennessey "Rule 41: Resolving Procedural Debates to Face the Tough Questions on Government Hacking" (1 December 2016) Lawfare < www.lawfareblog.com >; Kate Conger "Senators introduce bill to block controversial change to government hacking rule" (19 May 2016) Tech Crunch < www.techcrunch.com >; Jeff John Roberts "FBI's New Hacking Powers Take Effect This Week" (30 November 2016) Fortune < www.fortune.com >; Stuart Lauchlan "US Rule 41 makes data sovereignty even more complicated for cloud buyers" (5 December 2016) Diginomica < www.diginomica.com >; Joe Uchill "Last-ditch effort to prevent changes to law enforcement hacking rule fails" (11 November 2016) The Hill < www.thehill.com >.

87 United States Department of Justice "Mythili Raman Letter to Advisory Committee on the Criminal Rules" (18 September 2013) at 5, available at < <https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf> >.

88 In December 2016, the Home Office invited the Law Commission of England and Wales to conduct a one-year review to identify and address pressing problems with the law governing search warrants and to produce reform that will clarify and rationalise the law. For further information, see < www.lawcom.gov.uk/project/search-warrants/ >.

form, this will permit a search for and seizure of a physical device, such as a computer or mobile phone. The reason for this concentration on the device is that the information accessible from the device (as opposed to the device itself) is not a physical thing anchored to a unique location. It is therefore questionable both whether it is “on” the premises and whether it can be “seized” under section 8.

- 12.83 Independently of this power, whenever a police officer is lawfully on premises, whether under a search warrant or otherwise, there is a power under sections 19 and 20 of PACE to seize materials that they have reasonable grounds for believing to be evidence relevant to that or any other offence if they also have reasonable grounds for believing that there is a danger that the materials would otherwise be concealed, lost, altered or destroyed.
- 12.84 Section 19(4) of PACE states that the police officer may require “any information which is stored in any electronic form and is accessible from the premises to be produced in a form in which it can be taken away” if there are reasonable grounds to do so. This enables law enforcement officers to obtain data held on a different computer where the electronic information is accessible from a networked computer on the search premises.⁸⁹ There is some doubt about the meaning of “accessible from the premises” in section 19(4) because in one sense, all material on the Internet is accessible from any device anywhere in the world.
- 12.85 In relation to the issue of jurisdiction, Ian Walden notes that while section 19(4) does not have an explicit jurisdictional limitation, investigating officers may be in breach of unauthorised access offences in other jurisdictions if they conduct trans-border searches of data. He explains:⁹⁰

In all cases, the exercise of police powers are subject to the jurisdictional limitation placed on the police under [section 30(1) of] the Police Act 1996: “A member of a police force shall have all the powers and privileges of a constable throughout England and Wales and the adjacent United Kingdom waters.”

As a consequence of the jurisdictional limitation, investigators are obliged to give mind to the legality of any extra-territorial activity, since evidence obtained unlawfully from a foreign state may be excluded by a court either as an abuse of process or through the exercise of statutory discretion. However, prior to such a decision, the court would first need to determine whether to characterise police access as a territorial or extra-territorial exercise of power; then whether the activity is unlawful, under domestic or foreign law, either through breach of specific provisions, such as unauthorised access, or based on general principles of breach of national sovereignty and the comity of nations implied in the operation of such principles.

Australia

- 12.86 It is also not entirely clear whether trans-border access to data is permissible in Australia. Section 3L(1) of the Crimes Act 1914 (Cth) allows an officer who is executing a search warrant to use electronic equipment to access data if they suspect that it constitutes evidential material. The section reads as follows:

3L Use of electronic equipment at premises

- (1) The executing officer of a warrant in relation to premises, or a constable assisting, may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she suspects on reasonable grounds that the data constitutes evidential material.

89 Ian Walden “Computer Crime” in C Reed and J Angel (eds) *Computer Law* (Oxford University Press, Oxford, 2003) 295 at 8.7.2 and *Halsbury’s Laws of England* (online ed, LexisNexis) at [693].

90 Ian Walden “Computer Crime” in C Reed and J Angel (eds) *Computer Law* (Oxford University Press, Oxford, 2003) 295 at 8.7.2.

12.87 The author of *Cybercrime: Legislation, Cases and Commentary* notes that the phrase “including data not held at the premises” suggests a degree of latitude is to be afforded in executing the warrant. The author goes on to state that, taken literally, the words of the provision would allow cross-border Internet searches under Australian law.⁹¹ The Explanatory Memorandum associated with section 3L(1), however, indicates that this provision was inserted into the Act to enable access to business computer networks that extend across different office locations.⁹²

The Budapest Convention

12.88 The best evidence of State practice in this area, however, is the Council of Europe Convention on Cybercrime, otherwise known as the Budapest Convention.⁹³ This Convention is the leading international instrument relating to trans-border access to data. It has not been ratified by New Zealand, but it has been ratified by 54 countries including the United Kingdom and most other European Union countries, the United States, Australia and Canada.

12.89 The Budapest Convention requires State parties to legislate to ensure that all data that is accessible from an electronic device and is stored “in its territory” can be searched for law enforcement purposes.⁹⁴ The Convention then states that trans-border access to “stored computer data” can occur in two circumstances. Article 32 states:

Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

12.90 Significantly, the parties to the Budapest Convention are in the process of discussing several issues associated with trans-border access to data, including whether to extend article 32.⁹⁵ These discussions are focusing on the increasing “loss of location” of data; the ineffectiveness of current mutual legal assistance agreements in meeting time-sensitive requests from law enforcement agencies; and the uncertain role and inconsistent practices of major service providers.⁹⁶ These concerns are the same ones that were raised with us by enforcement agencies in their submissions.

12.91 In September 2016 the Cybercrime Convention Committee released a report, *Criminal Justice Access to Electronic Evidence in the Cloud*. The Report observes that:⁹⁷

91 Gregor Urbas *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths, New South Wales, 2015) at [11.7].

92 Cybercrime Bill 2001 (explanatory memorandum) at 17.

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

94 Article 19(2).

95 See Cybercrime Convention Committee *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for consideration by the T-CY* (September 2016) [*Criminal Justice*]. In relation to art 32, see Council of Europe *Explanatory Report to the Convention on Cybercrime 2001 ETS 185* (adopted 8 November 2011) at 293: “The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of the instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules”.

96 *Criminal Justice*, above n 95; and Osula “Transborder access”, above n 76, at 720.

97 *Criminal Justice*, above n 95, at [45].

It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of a suspect but also connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country.

12.92 In relation to this practice, the Report states:⁹⁸

... in the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote trans-border searches either formally or informally with unclear safeguards. Such unilateral or rogue assertions of jurisdiction will not be a satisfactory solution.

12.93 The Report contains a package of recommendations, all designed to address the various issues raised by cloud computing. One of the recommendations is that the parties to the Budapest Convention should negotiate a new protocol and that the following options for dealing with trans-border access to data should be considered:⁹⁹

- Permitting trans-border access without consent but with lawfully obtained credentials. The Report states that the other country would need to be notified before, during or after the event.
- Permitting trans-border access without consent in good faith (for example where the trans-border access occurs by mistake or by accident) or in exigent or other circumstance (for example where the access is necessary to prevent imminent danger, physical harm, the escape of a suspect or the destruction of evidence). The Report explains that, again, the other country would need to be notified.
- Using the “power of disposal” or the “person in possession or control” as the connecting legal factor. This option is built on the premise that “[e]ven if the location of data cannot be clearly determined, data can be connected to a person having the power to ‘alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever’”.¹⁰⁰

12.94 The Report states that these options would need to be subject to “specific conditions and safeguards”.¹⁰¹ On 8 June 2017, the Committee decided to initiate the drafting of the new protocol.¹⁰²

Our view on the issue of jurisdiction

12.95 Enforcement agencies stressed to us that officers may not know, and cannot be expected to know, where data is physically located in advance of a search. Even users do not tend to know where their data is stored. The agencies emphasised that increasingly data is stored overseas and the use of technology to aid concealment is on the rise. Law enforcement tools need to be able to combat these developments. Submitters also commented that irrational distinctions arise if data that is stored outside of New Zealand is inaccessible.

12.96 Despite these practical concerns, it is evident from State practice that the location of underlying data still matters to the international community. This means that enforcement officers do need to consider whether data is stored outside of New Zealand prior to searching it.

98 At [143].

99 At [144].

100 At [144].

101 At [144].

102 “Cybercrime: Towards a Protocol on evidence in the Cloud” (8 June 2017) Cybercrime Convention Committee News < <https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud> > .

- 12.97 If an enforcement agency cannot determine where the data is located, it is legitimate for it to conclude that the location is unknowable. In those circumstances, we consider that the Act should enable enforcement officers to access the data pursuant to a search warrant. In this respect, we endorse the Law Commission’s conclusion in 2007 that, while principles of territorial sovereignty should be recognised to the maximum extent possible, those principles are impossible to observe where the identity of the relevant jurisdiction is unknown.¹⁰³ This is the rationale that underlies the current remote access provisions in the Act and we are not convinced that there is a need to reverse that policy.
- 12.98 From an international perspective, that rationale is the most prevalent justification for trans-border access to data.¹⁰⁴ New Zealand therefore is unlikely to raise any international relations concerns by continuing to adopt this stance. That said, data stored in an “unknown location” will probably be the most common type of data that is of interest to law enforcement agencies in the future. As such, it would be preferable to be part of an international response to this issue.
- 12.99 The more difficult category is data stored in a known overseas location. In relation to this type of data, our primary recommendation is to firmly support the Law Commission’s original recommendation that consideration should be given to acceding to the Budapest Convention.¹⁰⁵
- 12.100 Trans-border access to data is an international issue. It cannot be resolved unilaterally. If New Zealand is a party to the Convention, it will be in a position to better understand, and influence, the coming developments. This includes planned improvements to the international co-operation regime,¹⁰⁶ which already provides for expedited preservation and access to stored computer data and requires all State parties to have a point of contact that is available 24 hours a day, seven days a week.¹⁰⁷ Accession to the Convention would also provide broader benefits to law enforcement.¹⁰⁸
- 12.101 The Convention is clearly still current. All of the countries that New Zealand traditionally compares itself to are parties, including all of our partners in the “Five Eyes” intelligence alliance.¹⁰⁹ In total, 55 countries have ratified the Convention and ten of those ratifications occurred in the last two years.¹¹⁰ Given the ease with which data can cross international borders it is important that New Zealand forms a co-operative relationship with the widest range of countries possible.
- 12.102 Further, as we will explain in Chapter 14, some of the parties to the Convention are currently discussing complementary agreements regarding the extraterritorial application of production orders.¹¹¹ These orders can be addressed to companies that store data in the ordinary course of their business, like Google and Facebook. The orders can be used to require the company to

103 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.123].

104 For instance, Rule 41 in the United States appears to be based on this justification.

105 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) recommendation 7.13.

106 Budapest Convention, Title 3 deals with international co-operation and the planned improvements are discussed in *Criminal Justice*, above n 95.

107 Budapest Convention, arts 29, 30, 31 and 35.

108 For instance, the Convention also provides for mutual assistance in relation to interception in arts 33 and 34.

109 That is, Australia, the United Kingdom, Canada and the United States.

110 *Ratified*: Albania (2002), Croatia (2002), Estonia (2003), Hungary (2003), Lithuania (2004), Romania (2004), Slovenia (2004), The Former Yugoslav Republic of Macedonia (2004), Bulgaria (2005), Cyprus (2005), Denmark (2005), Armenia (2006), Bosnia and Herzegovina (2006), France (2006), Netherlands (2006), Norway (2006), Ukraine (2006), United States (2006), Finland (2007), Iceland (2007), Latvia (2007), Italy (2008), Slovak Republic (2008), Germany (2009), Republic of Moldova (2009), Serbia (2009), Azerbaijan (2010), Montenegro (2010), Portugal (2010), Spain (2010), Switzerland (2011), United Kingdom (2011), Australia (2012), Austria (2012), Belgium (2012), Georgia (2012), Malta (2012), Japan (2012), Czech Republic (2013), Dominican Republic (2013), Mauritius (2013), Luxembourg (2014), Panama (2014), Turkey (2014), Canada (2015), Poland (2015), Sri Lanka (2015), Andorra (2016), Liechtenstein (2016), Israel (2016), Chile (2017), Greece (2017), Monaco (2017), Senegal (2017) and Tonga (2017). *Signed but not yet ratified*: South Africa (2001), Sweden (2001), Ireland (2002), San Marino (2017).

111 Chapter 14 at paragraphs [14.151]–[14.159].

provide electronic copies of relevant data to an enforcement officer rather than the officer using the Internet to access the data directly. Extraterritorial production orders would provide an alternative method for New Zealand enforcement agencies to access data that is stored overseas. Being a party to the Convention is likely to assist New Zealand in entering those discussions as well.

12.103 Finally, we note that one of the main reasons why New Zealand has not yet acceded to the Budapest Convention is the fact that the Convention requires each State party to have a preservation regime. This must enable data to be preserved pending the execution of a search warrant or a production order. We discuss this issue in Chapter 14 and recommend that a limited preservation regime should be enacted.¹¹²

RECOMMENDATION

R44 The Government should consider whether New Zealand should accede to the Council of Europe Convention on Cybercrime ETS 185 (Budapest Convention).

THE INTERNET SEARCH PROVISIONS IN THE ACT

The definition of “computer system”

12.104 As we explained at the start of this chapter, section 110(h) of the Act enables an enforcement officer executing a search warrant to use any reasonable measures to access “a computer system or other data storage device” that may contain evidential material. The recommendations we have made so far do not affect what is considered to be part of the device. As such, the definition of “computer system” is, and would remain, crucial to the statutory scheme. It provides the boundaries for digital searching.

12.105 The Act defines “computer system” as:¹¹³

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

¹¹² Chapter 14 at paragraphs [14.127]–[14.150].

¹¹³ Search and Surveillance Act 2012, s 3(1). Section 3(2) then clarifies: “For the purposes of the definition of computer system, a computer is interconnected with another computer if it can be lawfully used to provide access to that other computer—(a) with or without access information; and (b) whether or not either or both computers are currently turned on; and (c) whether or not access is currently occurring”. This clarification could be read as supporting either the narrow or broad interpretation of “computer system” discussed in this chapter.

- 12.106 The word “computer” is not defined in the Act but almost certainly includes mobile phones and tablets.¹¹⁴ As we explained in our Issues Paper, the definition of the wider term “computer system” is open to two, quite different, interpretations.¹¹⁵ This depends on how the word “interconnected” is understood.
- 12.107 If the interconnection is assessed from the perspective of an administrator or controller, two computers are interconnected if that person has the authority and the ability to determine how those computers will operate. The most common form of this type of interconnection is a “local area network”. A local area network consists of several linked computers, which together may provide computer services for a company, government agency or other organisation. Put simply, on the narrow interpretation, a “computer system” is akin to a local area network.
- 12.108 In contrast, the broad interpretation assesses whether the two computers are interconnected from the perspective of a user. A computer user can connect to millions of other computers through the Internet. Therefore, on this interpretation, a “computer system” includes any data that is accessible from the computer, including by use of the Internet. As we have discussed this data may be stored on an overseas server.
- 12.109 It is not clear from the rest of the definition whether the narrow or broad interpretation of “interconnected” is appropriate. The inclusion of “communication links” seems to support the broad interpretation because the phrase is so expansive. On the other hand, there would be no need to expressly include this phrase if “interconnected” already includes any possible form of connection.
- 12.110 There is no case law directly on point, and commentators are divided. The commentary to the Act in *Adams on Criminal Law – Rights and Powers* observes that the broad interpretation of “computer system” is available on the face of the statute.¹¹⁶ The same definition, however, is included in the Crimes Act 1961.¹¹⁷ The commentary on that definition in *Adams on Criminal Law – Offences and Defences* suggests that the narrow interpretation should be preferred primarily because that interpretation makes more sense in the context of the offence provisions in the Crimes Act.¹¹⁸ The author of *Internet.law.nz* also favours the narrow interpretation.¹¹⁹

114 This point has not been the subject of appellate scrutiny in New Zealand, as usually there is no need to distinguish between “computer system” and “other data storage device”. The legislative history and case law make it plain that mobile phones and tablets are covered by one, if not both, of these phrases (Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.4] and the cases at n 38 above). Presumably, however, the definition of “computer system” would need to be relied upon in order to claim that online data accessible through the phone is covered by a warrant or warrantless power. The phrase “other data storage device” would not, on its face, include interconnected devices/communication links. Our view is that, in ordinary usage, smartphones and tablets are more similar to a computer than a storage device. For further discussion, see Tania Singh and Nick Chisnall “Warrantless Searches of Electronic Devices” [2014] NZLJ 418 and David Harvey *Internet.law.nz* (4th ed, LexisNexis, Wellington, 2016) at [7.34].

115 Issues Paper, above n 31, at [6.88]–[6.98].

116 Simon France (ed) *Adams on Criminal Law – Rights and Powers* (online looseleaf ed, Thomson Reuters) at [SS3.09.01] and [SS110.12]. At [SS3.09.01] the authors state: “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”.

117 Crimes Act 1961, s 248. The Crimes Act was amended in 2003 to include this section and four others that relate to crimes involving computers.

118 See Simon France (ed) *Adams on Criminal Law – Offences and Defences* (online looseleaf ed, Thomson Reuters) at [CA248.04], where the authors state: “It is suggested the latter, narrower, meaning is more appropriate, not least because it allows a more discriminating approach to the concept of ‘authorisation’ which is a critical issue in relation to the offences created by s 250 [of the Crimes Act 1961 – damaging or interfering with a computer system], in that we may distinguish between systems to which a person may have leave or authority to access as a user or consumer from those systems to which the same person has access or authority in the capacity of operator or controller or as authorised by law or judicial warrant. It may also be argued that the inclusion of ‘communication links’ in other parts of the definition points to the narrower meaning as being correct since there would be no need to refer to communications links between computers if the broader meaning of ‘interconnected’ applied”.

119 David Harvey *Internet.law.nz* (4th ed, LexisNexis, Wellington, 2016) at [7.39]–[7.41] and [8.224]–[8.235]. At [7.41], the author specifically states: “The latter approach [which we have described as the narrow interpretation of “computer system”] is favoured. It allows a more critical approach to the issue of ‘authorisation’, especially having regard to offences under s 250 [of the Crimes Act 1961]. It is possible to distinguish between the systems to which a person may have authority to access as a user or consumer or as an operator or controller, or authorised by law or judicial warrant”.

- 12.111 The legislative history of the provision contains indicators that could be read in support of either interpretation. The first version of the Search and Surveillance Bill 2009 did not refer to “computer system” at all. Instead it allowed for a person executing a search power “to access and copy intangible material from computers and other data storage devices located at or accessible from” the relevant scene.¹²⁰
- 12.112 The Select Committee then suggested an amendment to this clause in accordance with a recommendation made by the Law Commission and Ministry of Justice in their departmental report. The departmental report advised that:¹²¹
- ... the use of the term *accessible from* is overly broad, and may permit access to a larger repository of information than intended. The provisions were intended to ensure that enforcement officers could search computers that are connected by a network, and information that a company stores on servers that are not located at the search premises.
- 12.113 To address this problem the departmental report recommended that the phrase “computer system” should be used and that the definition in the Crimes Act should be adopted.¹²² This supports the narrow interpretation.
- 12.114 However, the departmental report’s recommendation reflected the Law Commission’s original suggestion in its 2007 Report that the definition in the Crimes Act should be adopted.¹²³ That suggestion was accompanied by a statement that if a person accesses an Internet data storage facility from “a dedicated computer”, that facility should be viewed as part of the “computer system”.¹²⁴ This aligns more closely with the broad interpretation.
- 12.115 Regardless of what Parliament’s original intention was, it is clear that there is now confusion. The practice of enforcement agencies varies, and there is a pressing need for greater clarity, given the importance of this definition. This issue, however, cannot be examined in isolation. It is intimately connected to the remote access authorisation provisions in the Act. Therefore, we discuss those provisions before outlining our recommendations in paragraphs [12.125]–[12.153].

The remote access authorisation provisions

- 12.116 The Act empowers an enforcement officer to apply for a search warrant enabling the officer to conduct a remote access search.¹²⁵ This is defined 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”.¹²⁶ If a warrant is to authorise a remote access search, the application must contain “the access information that identifies the thing to be searched remotely”.¹²⁷ For example, this could be the username and password for an online account. Upon completion of a remote access search, the enforcement officer must send an email notification to the thing searched. There is no power in the Act to delay that notification.¹²⁸ There is also no power to conduct a warrantless remote access search.

120 Search and Surveillance Bill 2009 (45-1), cl 108(i).

121 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [412].

122 At [413]–[416].

123 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.92].

124 At [7.94].

125 Search and Surveillance Act 2012, ss 103(4)(k) and 111.

126 Search and Surveillance Act 2012, s 3(1).

127 Section 103(4)(k).

128 Section 132.

- 12.117 The remote access provisions were designed to respond to the growing tendency of Internet users to store their data on Internet data storage facilities (for example, Gmail), which are accessible from any device with Internet access.¹²⁹ The Law Commission explained in its 2007 Report that, in this situation, “there is no specific physical location that can practicably be searched to locate a device that can then be subjected to a computer search”.¹³⁰ The Commission also observed that—where data is stored on such facilities—it may be “entirely unclear in which jurisdiction accessible data is held”.¹³¹ In those circumstances, the Commission considered that enforcement officers should be permitted to obtain a warrant to access the data.¹³²
- 12.118 Whether the broad or narrow interpretation of “computer system” is adopted has a significant impact on how the remote access authorisation provisions are understood. If a computer system is limited to data stored within that computer’s local area network, a second warrant containing remote access authorisation must be obtained to conduct an Internet search. However, if the broad interpretation is adopted, online data that is accessible from the device is part of the computer system and can be searched without remote access authorisation.

Submissions

- 12.119 Our Issues Paper asked for submitters’ views on whether the provisions in the Act on remote access searches were sufficiently clear.¹³³ The general consensus was that the provisions are unworkable. Enforcement agencies identified three main problems. First, the requirement that an issuing officer must be “satisfied that the thing is not located at a physical address that a person can enter and search”¹³⁴ is illogical because technically all digital data is stored on a device or server *somewhere* and theoretically that location could be entered and searched. On this technical interpretation, it is impossible for an enforcement officer to demonstrate that this requirement is satisfied.
- 12.120 Second, it is unlikely that an enforcement officer will know the password for an online account at the time they apply for a search warrant. That information will often be obtained during the search (for example, if the user has set up the account to stay logged in on a particular device). This means that enforcement agencies rarely have enough information to seek remote access authorisation when they first apply for a warrant. They would need to apply for a second warrant once the access information is known, by which time any evidential material in the account may have been destroyed.
- 12.121 Third, compliance with the notice provisions is often impossible because not all things that may be the subject of a remote access search are associated with an email address. Even if such an address is available, it is not clear whether the user or the provider of the online account should be notified. Further, there is no obvious reason why there is no option to delay notification as there is for every other type of search.
- 12.122 The result of these problems is that, in practice, remote access search warrants are not sought by many agencies. Such searches seem to be limited to those cases where the enforcement agency wishes to conduct the search from its own office (which we refer to in this chapter as “remote execution”). In other cases, it appears that enforcement officers instead rely on the broad interpretation of “computer system” as discussed above. This allows an officer to access

129 See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.94].

130 At [7.94].

131 At [7.123].

132 At [7.123].

133 Issues Paper, above n 31, question 27.

134 Search and Surveillance Act 2012, s 103(6).

an online account from a computer that is covered by a search warrant. The officer can require the user to provide their username and password and the user is notified in real time.

- 12.123 This practice raises the concerns about jurisdiction that we discussed at paragraphs [12.71]–[12.103] above. If “computer system” is interpreted broadly as including any data accessible from the computer, a search can easily cross international borders. Several submissions highlighted this issue and argued that the Act should not give enforcement officers direct access to data that is stored overseas.
- 12.124 Submitters commented that trans-border access to data is, unavoidably, an international issue and should be dealt with by way of international agreements. It was suggested that New Zealand should not risk its international reputation by attempting to resolve these issues unilaterally. In response to this point enforcement agencies have advised us that current mechanisms for international co-operation are prohibitively time-consuming and resource-intensive. If those mechanisms were the only avenue of accessing data stored overseas, this would be crippling for law enforcement.

The case for reform

- 12.125 We consider that the definition of “computer system” in the Act is unclear and that the remote access search provisions, as currently drafted, are unworkable. These sections need to be amended to clearly explain how data that is readily accessible from a device, but not stored on the device, should be accessed by law enforcement. That data could be stored:
- on the device’s local area network;
 - not on the local area network but elsewhere in New Zealand;
 - outside of New Zealand in a known or knowable location; or
 - in an unknown or unknowable location.
- 12.126 We also consider that the Act should contain broader and clearer rules around when an enforcement agency can access stored data through an unrelated device, such as one of the agency’s own computers. This could arise in relation to any warrant authorising a digital search. We describe this as “remote execution”.
- 12.127 We prefer “remote execution” because we find the phrase “remote access” confusing. The phrase “remote access” suggests distance between the thing that is *accessing* and the thing that is being *accessed*. The thing being accessed is the data storage facility that has no physical location (in a general sense), but it is not clear who or what is accessing it. The focus could be the device being searched (which would fit with the narrow interpretation of “computer system” because the data is stored remotely from the device) or it could be on the searcher (which would suggest that there is no specific device being searched and that this is actually a remote execution provision). The meaning is not immediately apparent.
- 12.128 As noted in paragraph [12.122] above, the remote access search provisions are mainly used to enable remote execution of a warrant. However, we do not think that the provisions were intended to be used solely in this way, and therefore they do not provide a sufficiently transparent and complete set of rules around this activity. These matters need to be squarely addressed in the legislation given that, by definition, the owners of the relevant data are not present during the remote execution of a search warrant.
- 12.129 As we explain further below, we have formed preliminary views about how a new statutory regime to replace the remote access search provisions could be framed. However, there are

technical matters that still need to be resolved so our recommendations in this regard are provisional in nature.

A revised definition of “computer system”

- 12.130 During the consultation process, we proposed the option of re-defining “computer system” with reference to local or wide area networks.¹³⁵ This option seemed to be most in line with Parliament’s original intentions. We have concluded, however, that this approach would give rise to technical issues and would potentially cause greater confusion. The terms “local area network” and “wide area network” are already becoming outdated.
- 12.131 We have also formed the view that there is no real need for the definition of “computer system” to distinguish between data stored on a local area network and other data that is stored in New Zealand. What matters is that the data is accessible from the device and is within New Zealand’s territorial jurisdiction. To reflect that, we considered adding a geographical limitation to the definition of “computer system”. This would limit the definition to computer systems or the parts of computer systems that are in New Zealand. This would be similar, in effect, to the approach that seems to be taken in the United Kingdom.¹³⁶
- 12.132 We questioned, however, whether this would be workable in practice given that it is very difficult for enforcement agencies to pinpoint exactly where data is stored. To get around this problem, we reflected on the fact that law enforcement agencies generally disconnect electronic devices from the Internet when they commence a search, in order to preserve the integrity of the data that existed at the time of the search. If a device is disconnected from the Internet, an enforcement officer could have some confidence that the remaining accessible data is stored in New Zealand. We understand, however, that this will not always be the case. Devices can connect to other wireless or wired networks that can access data that is stored overseas. By way of example, some businesses may have wide area networks that can access data stored in Australia without the use of the Internet. Accordingly, while disconnecting a mobile phone or a personal computer may provide reassurance that the remaining “computer system” is in New Zealand, that may not be the case if a search of networked computers in a workplace is involved.
- 12.133 We have not had time to explore these options in any detail with the technical experts within enforcement agencies. Consultation with such experts is necessary to determine exactly how hard it would be to identify whether data accessible from an electronic device is stored in New Zealand, in a range of different scenarios. The technical experts are also best placed to provide advice on whether our proposals may have unintended consequences and whether those consequences could be avoided. Without having had those discussions, we do not think that it would be appropriate to make firm recommendations. We do, however, think that further consideration should be given to whether the definition of “computer system” in the Act:
- should be limited so that it only covers computer systems or the parts of computer systems that are in New Zealand; and
 - should expressly exclude data that is only accessible when the device is connected to the Internet.
- 12.134 The benefit of expressly excluding data that is only accessible when the device is connected to the Internet is that it would make the parameters of the “computer system” narrower (to more closely resemble a local or wide area network) and more discernible. In most cases,

135 A wide area network is a computer network that covers a broad geographical area and that may include some local area networks.

136 See the discussion in paragraph [12.84].

disconnecting the device from the Internet would also resolve the jurisdiction concern. In other cases (where wide area networks may be involved) we acknowledge that the officer would need to take further steps to determine the limits of the “computer system”.

Internet access authorisation

- 12.135 Given the increase in internet usage and cloud computing, it is important for enforcement officers to be able to readily search data that is accessible from a device using the Internet, and that is stored in New Zealand or an unknown location. As we have explained, such Internet searches do not appear to engage significant concerns about jurisdiction and they are necessary for effective law enforcement. To facilitate that process we think consideration should be given to whether the Act should be amended to include an Internet access authorisation regime.
- 12.136 The Internet access authorisation regime would require an enforcement officer to obtain prior authorisation from an issuing officer to conduct an Internet search. This authorisation would be obtained as part of the process of applying for a warrant to search an electronic device. If the officer considered that the stored data they are looking for may only be accessible from the device using the Internet, this matter can be raised with the issuing officer at the outset. We do not think that it would be appropriate to require the officer to search the device first and then to apply for a second warrant. That would unduly delay investigations, potentially leading to the loss of crucial evidence.
- 12.137 To obtain Internet access authorisation the search warrant application would need to contain the following:
- A description of the facility, data or other information to be accessed using the Internet that is as specific as the circumstances allow. For example, “any Dropbox account identified during the search of an electronic device as being used by person x”. The aim here is simply to identify the parameters of the Internet search.
 - Any necessary access information where known or, if not known, a description of how the access information will be obtained.
 - An explanation of why there are reasonable grounds to believe that evidential material will be found during the proposed Internet search.
- 12.138 This Internet access authorisation requirement would recognise the Internet as being a slightly different, albeit related, place that is being searched.¹³⁷ We do not think the Act should make it overly difficult to extend a warrant that relates to a device to a warrant that has Internet access authorisation. The Act needs to recognise how frequently information that could be stored on a device is now stored in the Cloud. Equally, however, Internet searches need to have identifiable boundaries just like any other search. In some ways, this is especially important for Internet searches because, as we explain below, individuals can be required by enforcement officers to provide the access information for their online accounts.¹³⁸ Before doing so, we think that the individual is entitled to see from the warrant that the search of the account has been authorised by an independent issuing officer.

¹³⁷ To clarify, we envisage that a warrant with Internet access authorisation could be issued in respect of “a place, vehicle or other thing” in accordance with s 6 of the Act and would identify the electronic devices and Internet sites that could be searched. By contrast, a warrant with remote execution authorisation (which we discuss below at paragraphs [12.145]–[12.148]) could be issued solely in respect of a “thing”, and that thing would need to be an Internet site or sites. This distinction has an impact on the notification requirements. We think that the ordinary requirements for notification in s 131 of the Act should apply to warrants with Internet access authorisation. Different rules for notification should apply to warrants with remote execution authorisation, as we discuss at paragraph [12.147].

¹³⁸ Search and Surveillance Act 2012, s 130.

- 12.139 We recognise that a difficulty with our proposed Internet access authorisation regime is that it would not clearly identify data that is stored in a known or knowable overseas location as being subject to different rules. As explained above, international law and State practice indicates that this data should only be accessed if it is publicly available or with the consent of the user or the other State. If it is not, there is a risk the enforcement officer will commit an offence in the foreign country, such as accessing a computer system without authorisation.¹³⁹ The additional steps required to obtain consent and/or authorisation from the foreign State would depend on the particular State involved. Some States are likely to require compliance with mutual assistance procedures.
- 12.140 To address this difficulty we considered requiring applications for Internet access authorisation to also include a statement that the applicant has taken reasonable steps to determine whether the data is held in an identifiable overseas location and has concluded that it is not. This would have the benefit of reversing the onus in the current remote access search provisions, which require the applicant to positively establish that the data is not in a place that can be entered and searched. By contrast, the additional requirement would start from a presumption that the data is in New Zealand or an unknown location. If the applicant did find that the data was in a known overseas location, the warrant process would not be the appropriate option. Instead the applicant would need to contact the Crown Law Office in the first instance to determine whether any relevant mutual assistance agreements were in place.¹⁴⁰
- 12.141 Enforcement agencies strongly opposed this additional requirement. They explained that it is simply too difficult to identify where data is stored. A statutory requirement to take reasonable steps to do so would divert precious resources to a routinely futile task. There is force in this concern and we do not wish to recommend a proposal that would ultimately become little more than a box-ticking exercise. As cloud computing becomes increasingly common, it will become more unlikely that enforcement agencies will need to access data in known overseas locations.
- 12.142 In addition, we are cautious about suggesting the inclusion of a statutory requirement that reflects current international law and State practice but may not reflect any of the changes to that law and practice that are on the horizon.
- 12.143 We note that enforcement officers are already aware of the risks associated with accessing data that is known to be stored overseas. Further, section 30 of the Evidence Act 2006 may already provide a statutory safeguard. Like in the United Kingdom, it is at least arguable that evidence obtained in breach of a foreign offence provision and/or in breach of customary international law could be ruled inadmissible as improperly obtained evidence under section 30.¹⁴¹ However, we do not view this as an ideal long-term solution. As we explained in Chapter 2, it is better for issues that could affect the legality or reasonableness of a search to be dealt with upfront during the authorisation stage, rather than waiting for back-end validation through the admissibility process.¹⁴² Therefore, we think that further consideration should be given to this issue during the process of exploring the efficacy of our recommendations with technical experts.
- 12.144 In that regard, we note that an enforcement agency raised a concern with us that our proposed Internet access authorisation regime may impact on the ability of forensic searchers to

139 The equivalent offence in New Zealand is in s 252 of the Crimes Act 1961.

140 The Attorney-General is responsible for receiving and making requests for mutual assistance under the Mutual Assistance in Criminal Matters Act 1992. In practice, formal requests for assistance are received and made by the Crown Law Office on behalf of the Attorney-General. For a further discussion of how the mutual assistance process works in New Zealand see *Attorney-General v Dotcom* [2014] NZCA 19, [2014] 2 NZLR 629 and Law Commission *Modernising New Zealand's Extradition and Mutual Assistance Laws* (NZLC R137, 2016).

141 Section 30 of the Evidence Act 2006 is specifically being considered by the Law Commission in the context of its second statutory review of the Evidence Act, which commenced in February 2017. The Commission must report to the Minister of Justice by 20 February 2019.

142 Chapter 2 at paragraphs [2.73]–[2.74].

download tools from the Internet to assist in searching an electronic device or a clone of a device. We think that this matter could potentially be addressed through the drafting process, by including a specific exception. It should, however, be explored further.

Remote execution authorisation

- 12.145 As noted above,¹⁴³ our understanding is that in practice the remote access search provisions in the Act are currently used primarily to enable the remote execution of a warrant. This involves the enforcement agency conducting an Internet search from the agency's office. If the remote access search provisions are repealed, we consider that new and more transparent provisions should be enacted to enable an enforcement officer to remotely execute a search warrant. We therefore recommend that further consideration should be given to amending the Act to allow an enforcement officer to apply for a search warrant with remote execution authorisation. This authorisation would be obtained as part of the process of applying for the warrant.
- 12.146 We envisage that an application for a search warrant with remote execution authorisation would need to contain the following:
- A precise description of the thing to be searched. The reason for this requirement is that the authorisation will relate to an Internet search and the “thing” to be searched (in terms of the criteria for a search warrant in section 6) will not be able to be identified by reference to an associated device. The “thing” will be a facility, data or access information. In those circumstances the warrant application will need to contain a more precise description of the thing to be searched than is required when simply seeking Internet access authorisation. For Internet access authorisation a broad description may suffice depending on the circumstances of the case. For example, it may be sufficient to identify: “any Gmail account that person x’s laptop automatically populates the access information for when the Gmail website is opened using the device”. For remote execution authorisation, however, the applicant would need to provide the username and password for the Gmail account.
 - An explanation of why remote execution is an available and reasonable option in the circumstances of the case.
 - A description of how the applicant intends to notify the user of the device, facility, data or information.
 - If the applicant is seeking a deferral of notification, an explanation of why deferral is justified.
- 12.147 In terms of the notification requirements, we are conscious that where a warrant is remotely executed, the user/occupier will never be present. In those circumstances, we consider that the warrant should contain a detailed explanation of how notification will occur. We also consider that there should be an ability to apply to a Judge to defer, further postpone or obtain a dispensation from the notification requirements if compliance would endanger the safety of any person or prejudice ongoing investigations. This option is available in respect of other search powers and we see no reason to distinguish remotely executed Internet searches in this regard.¹⁴⁴
- 12.148 Finally, we note that the issue of data being stored in a known or knowable overseas location also arises in relation to remotely executed Internet searches.

¹⁴³ Chapter 12 at paragraph [12.122].

¹⁴⁴ Search and Surveillance Act 2012, ss 134 and 135.

A warrantless power to continue a search using the Internet

- 12.149 An enforcement officer executing a search warrant may well come across information that suggests the data the officer is actually looking for is stored in a location that is accessible using the Internet but not covered by the warrant.¹⁴⁵ Given the nature of the digital environment it would be virtually impossible to preserve the data in this location pending a second warrant, as internet-based data can be altered or deleted from anywhere. We understand that any attempt to change the access information and lock the user out could easily be countered. To reflect that reality, we suggest the Act could be amended to include a new warrantless power to initiate an Internet search (if the warrant only related to a device) or to extend an Internet search (if the warrant already enabled an Internet search either through Internet access authorisation or remote execution authorisation).
- 12.150 The warrantless power would only be available if, during the execution of the search warrant, the executing officer becomes aware of new information and forms a reasonable belief that evidential material will be destroyed before a second warrant can be obtained. The basis for this belief would need to be case-specific. The ease with which data can be deleted online would not, in itself, be sufficient.
- 12.151 By way of example, it would be appropriate to exercise the warrantless power if, during the remote execution of a search warrant, the officer becomes aware that new relevant data exists but the owner of the data is in the process of deleting it. It may not be sufficient if, in the same example, there was no indication that the owner of the newly identified data intended to destroy it.
- 12.152 As mentioned in paragraph [12.68] above, we suggest that this new warrantless power be subject to a record-keeping requirement. This could be achieved by amending section 169(3) of the Act, which already requires certain information to be internally reported when a warrantless power has been exercised. We understand that these internal reports are routinely disclosed to defence counsel. Therefore the requirement to record the search procedure would provide additional accountability.
- 12.153 We also note that, since this warrantless power is predicated on the initial search being conducted pursuant to a warrant, there would be no ability to combine the power with the warrantless power to search an electronic device in urgent circumstances that is recommended in paragraph [12.42]. That power already enables an Internet search, but only to prevent offending or respond to risks to life or safety – not to preserve evidence. The two warrantless powers are therefore mutually exclusive.

145 As explained in paragraph [12.42], we recommend that the warrantless power to search an electronic device in urgent situations should also enable an enforcement officer to connect that device to the Internet. The warrantless power is designed to assist in preventing offending or responding to a risk to life or safety. It has no evidence-gathering purpose.

RECOMMENDATION

- R45 The Ministry of Justice should give further consideration to the following:
- (a) Whether the remote access search provisions in the Act should be repealed.
 - (b) Whether the definition of “computer system” in the Act should:
 - (i) be limited so that it only covers computer systems, or the parts of computer systems, that are in New Zealand; and
 - (ii) expressly exclude data that is only accessible when the device is connected to the Internet.
 - (c) Whether provisions should be inserted into the Act to require an enforcement officer to obtain a search warrant with Internet access authorisation before accessing the Internet during a search.
 - (d) Whether provisions should be inserted into the Act to allow an enforcement officer to obtain a search warrant with remote execution authorisation. This authorisation would enable a search warrant that only relates to an Internet search to be executed remotely.
 - (e) Whether provisions should be inserted into the Act to enable an enforcement officer conducting a digital search pursuant to a search warrant to extend that search to internet-based data not specified in the warrant, by exercising a new warrantless power, if they have reasonable grounds to believe:
 - (i) that evidential material relating to the offence is in a place that can be accessed using the Internet; and
 - (ii) that, in the particular circumstances of the case, if access is delayed to obtain a second search warrant, the evidential material will be destroyed, concealed, altered or damaged.

The warrantless power should be subject to a requirement to document the search procedure during or as soon as practicable after the search.

ACCESS INFORMATION

- 12.154 Up until this point we have discussed the types of warrants and warrantless powers that should be available in respect of digital searches. However, once an enforcement officer has obtained lawful authority to search an electronic device or an online account, a separate issue arises in relation to how the data within it is accessed.
- 12.155 As we discussed in Chapter 2, in recent years there has been a significant growth in encryption technologies that hinder law enforcement’s access to devices and online accounts.¹⁴⁶ By “encryption” we mean the process of encoding data or information in a way that is intended to prevent access to that data by any unauthorised person. Two major developments have taken place:
- manufacturers of electronic devices are adopting operational systems that encrypt information by default; and

¹⁴⁶ Chapter 2 at paragraphs [2.56]–[2.59].

- service providers are increasingly offering automatic encryption of data stored in cloud storage systems of a kind that prevents even the service providers from being able to decrypt the data.
- 12.156 Due to these developments, law enforcement agencies around the world are increasingly struggling to access data held on electronic devices and in online accounts, even when they have lawful authority to do so in the form of a warrant.¹⁴⁷
- 12.157 We consider that, if an electronic device or online account is the subject of a search warrant, the Act should provide law enforcement officers with meaningful and appropriate tools to lawfully obtain the necessary passwords, encryption keys and other access information. Without such tools, these warrants would be redundant.
- 12.158 Sections 130 and 178 of the Act were designed to assist in this regard. These provisions make it an offence to refuse to provide an enforcement officer with access information for a device or Internet site that is the subject of a lawful search without a reasonable excuse. The maximum penalty for this offence is three months' imprisonment.¹⁴⁸
- 12.159 In our Issues Paper we identified two problems with these provisions:¹⁴⁹
- it is not clear how the privilege against self-incrimination relates to the offence; and
 - the relatively low maximum penalty may not motivate compliance.

The privilege against self-incrimination

- 12.160 Section 130 of the Act is drafted in a confusing manner. We explained this in our Issues Paper, and all eight of the submissions we received on this point agreed.¹⁵⁰
- 12.161 In brief, section 130(1) enables an enforcement officer to require a specified person to provide access information or other assistance to access a device or Internet site. Section 130(2) then explains that a specified person may not be required “to give any information tending to incriminate the person”. Section 130(3) clarifies that the enforcement officer may nonetheless ask for the access information even if the device may contain “information tending to incriminate the specified person”. This implies that the protection in section 130(2) remains where the access information, in itself, is incriminating. However, that is not expressly stated, unlike in section 198B of the Summary Proceedings Act 1957 (now repealed), which was the predecessor to this section.¹⁵¹
- 12.162 To add to the confusion, section 130(4) of the Search and Surveillance Act states that subsections (2) and (3) are subject to subpart 5 of the Act. Subpart 5 relates to privilege and confidentiality. It is hard to see how any of the provisions in subpart 5 could be relevant to section 130 except, potentially, those relating to the privilege against self-incrimination. Subpart 5, however, states that this privilege may only be claimed in response to a production

147 This phenomenon is described as “going dark” and has been the subject of considerable public debate in the United Kingdom and the United States over the past two years. The difficulties posed by the rise in encryption are not limited to searches of stored data. The debate is also focused on surveillance capabilities. The central issue is whether companies should be required by law to build “back door” access for law enforcement to communications data. This proposal was met with widespread criticism, largely on the basis that it will compromise the overall security of data communications. See Berkman Center for Internet and Society *Don't Panic: Making Progress on the “Going Dark” Debate* (Harvard University, 1 February 2016) and Chertoff Group *The Ground Truth about Encryption: And The Consequences of Extraordinary Access* (2016).

148 Search and Surveillance Act 2012, s 178.

149 Issues Paper, above n 31, at [8.70] and [6.131].

150 At [8.66]–[8.75].

151 Summary Proceedings Act 1957, s 198B(4)(b) included the phrase “does not in itself tend to incriminate the person”.

or examination order.¹⁵² It is uncertain what effect this was intended to have on the protection in section 130(2).

- 12.163 The result is that it is not clear whether a specified person can refuse to provide access information, such as a password, on the basis that:
- the content of the password is incriminating (for example, the password is “I murdered Joe Bloggs”);
 - knowledge of the password is incriminating (for example, in a case where ownership or use of the device or Internet site is likely to be in dispute); and/or
 - the act of providing the password is incriminating because it will lead to the discovery of incriminating evidence.
- 12.164 In our Issues Paper, we suggested that one option for resolving this confusion was to amend section 130(3) of the Act to clarify that a specified person does not need to provide access information that “in itself tends to incriminate” that person. On reflection we consider that this phrase is ambiguous. It clearly covers incriminating content but, arguably, it could cover incriminating knowledge as well. Accordingly, the amendment would not promote greater clarity. It also would not resolve the issue of the relevance of subpart 5.
- 12.165 Further, the consultation process highlighted to us that this is more than just an issue of drafting. There was extensive division amongst submitters and those we consulted with as to whether the privilege should be available in each of the three scenarios described in paragraph [12.163] above. In particular, there was divided opinion on whether a person should be required to admit to knowing how to access a device or Internet site. It was suggested that, as a compromise, the Act could be amended to state that if a person assists in accessing a device or site then the fact of that assistance may not be used as evidence against them in court. In our opinion no such compromise is necessary.
- 12.166 In New Zealand, the privilege against self-incrimination is governed by section 60 of the Evidence Act 2006. That section explains that the privilege applies when a person is required by an enforcement officer to provide specific information that is likely to incriminate them during a criminal investigation.¹⁵³ For the purpose of this section, the Evidence Act defines “information” as a statement given orally or in a document prepared afterwards and in response to the request.¹⁵⁴ The history of this definition is illuminating.
- 12.167 In 1996¹⁵⁵ and 1999,¹⁵⁶ the Law Commission released two publications concerning evidence law reform, both of which looked at an analogous issue of whether a person could refuse to produce documents pursuant to a statutory power of compulsion on the basis that they would have to reveal that they knew the documents existed and/or where they were. A 1986 New Zealand Court of Appeal case and various United States authorities recognised that the privilege against self-incrimination could attach to this type of “non-verbal assertion”.¹⁵⁷ The

152 Section 136(1)(g) recognises the privilege against self-incrimination as described in s 60 of the Evidence Act for the purposes of subpart 5 but “to the extent provided in s 138, and only to that extent”. Section 138 appears under the heading “examination and production orders”. Section 138(1) explains that examination orders and production orders do not affect the privilege against self-incrimination that a person may have under s 60 of the Evidence Act 2006. The remainder of the section then explains the process for claiming the privilege and resolving the matter in the District Court if necessary.

153 Evidence Act 2006, s 60(1)(a)(iii).

154 Evidence Act 2006, s 51(3).

155 Law Commission *The Privilege against Self-Incrimination: A Discussion Paper* (NZLC PP25, 1996).

156 Law Commission *Evidence: Reform of the Law* (NZLC R55 Vol 1, 1999).

157 Law Commission *The Privilege against Self-Incrimination: A Discussion Paper* (NZLC PP25, 1996) at [202] citing *New Zealand Apple and Pear Marketing Board v Masters & Sons Ltd* [1986] 1 NZLR 191 (CA) at 194–195, *Fisher v United States* 425 US 391 (1976) at 402–414 and *Doe v United States* 487 US 201 (1988) at 209.

- Commission concluded that it would be “illogical” for documents to be compellable under a production order but for the person to be able to resist the act of compulsion on the basis of privilege.¹⁵⁸ For that reason, the Commission suggested that the definition of “information” in the Evidence Act should be limited to oral statements and documents made in response to a request.¹⁵⁹ “Non-verbal assertions” were specifically left out.¹⁶⁰
- 12.168 Drawing on that reasoning, we think it is plain that the privilege against self-incrimination should not be available simply because the assistance will lead to the discovery of incriminating evidence. Nor should it be available to protect a person from having to disclose the fact that they know what the access information is. That fact is an inference drawn from the provision of existing information as opposed to an oral statement or document created in response to a request for information. Therefore, the privilege against self-incrimination as recognised by section 60 of the Evidence Act does not apply in this situation. Given that, we do not think there is any reason to place restrictions on the use of that fact as evidence at trial.
- 12.169 We recommend that the privilege against self-incrimination should only be available under section 130 of the Act if it is the *content* of the access information that is incriminating. In such cases, the Act should permit a privilege claim to be made. The validity of that claim would then need to be determined in court (or by an out-of-court arrangement agreed upon by the parties).¹⁶¹ We envisage that successful privilege claims of this kind would be extremely rare. Where a successful claim is made, it would only justify a refusal to provide the access information to an enforcement officer. The enforcement officer could still require the person to provide other assistance to access the device or Internet site, such as by entering the access information directly.
- 12.170 Our recommendation aligns with the original policy behind section 130. Clarification of that policy will strengthen the tools available to law enforcement by reducing the likelihood of unmeritorious privilege claims and by making it clear that even a successful claim does not prevent the provision of other forms of assistance.
- 12.171 In terms of drafting, we suggest that the provision could state that an enforcement officer may require a person to provide any assistance that is reasonable and necessary to access a device or an Internet site. In other words, the express reference to the provision of “access information” would be removed. This would avoid a presumption that access information must be provided orally or in writing in order to comply with the section. In many cases, the requirement to provide assistance could be satisfied by the person directly entering their access information into the device or site.
- 12.172 There may, however, be other cases where it is reasonable and necessary for the access information to be provided orally or in writing, for instance if the officer needs to search a device off-site. It is only in those situations that the Act should provide an avenue for claiming the privilege against self-incrimination.

158 Law Commission *Evidence: Reform of the Law* (NZLC R55 Vol 1, 1999) at [281].

159 At [281].

160 Notably, s 103(3)(b)(ii) of the Act states that a search warrant can contain a condition that an occupier must provide reasonable assistance to the person executing it, if in the absence of the assistance there would be undue delay. This seems to relate to things like physically providing a key. Section 103(7) then clarifies that a person is not required by such a condition to “give any information tending to incriminate the person”. Presumably this relates to oral statements and the creation of documents, and not “non-verbal assertions” like unlocking a door, as that is not “information”.

161 We discuss out-of-court privilege claims and privilege generally in Chapter 17 at paragraphs [17.24]–[17.30].

The maximum penalty

- 12.173 Since the enactment of the Search and Surveillance Act, Police has initiated 33 prosecutions against individuals who refused to provide access information and other information or assistance when required to do so under section 130. We were told that such refusals are prematurely ending investigations. In our Issues Paper, we questioned whether an increase to the maximum penalty of three months' imprisonment could increase the rate of compliance.¹⁶² We put forward the option of including a fine of up to \$10,000. This amendment would clarify that a financial penalty could be imposed instead of imprisonment.¹⁶³
- 12.174 The majority of submitters agreed that the penalty provision should expressly include the option of a fine. It was noted, however, that this probably would not affect the rate of compliance. Several submitters commented that, unless the penalty for failing to assist is higher than any offence a person may be trying to conceal, there is no incentive to co-operate. This is true but is also an inevitable reflection of the presumption of innocence. If a person is presumed not to have committed an offence, it is illogical to punish them as if they had committed the offence purely because they chose not to provide access information. There could be a variety of explanations for that choice.
- 12.175 We do not think the primary solution to the problem of non-compliance with section 130 lies with an amendment to the maximum penalty. Rather, we consider that new tools need to be available to allow enforcement agencies to lawfully obtain access information by other means. That is one of the rationales behind our recommendation in Chapter 7 that the Act should be amended to enable the use of data surveillance technology, including keystroke logging software.
- 12.176 We envisage that, in a sufficiently serious case,¹⁶⁴ a data surveillance warrant could be issued enabling an enforcement officer to obtain access information by installing keystroke logging software. We are conscious that warrants can only be issued to obtain "evidential material". We believe, however, that access information could qualify as evidential material. That is because the Act broadly defines this phrase to include any intangible item of relevance to the investigation.¹⁶⁵
- 12.177 Despite our conclusions above, we recommend an increase in the maximum penalty for failing to comply with a request under section 130. This recommendation flows from our recommendation at paragraphs [12.39]–[12.43] above that, except in cases of urgency, every search of an electronic device or an online account should be conducted pursuant to a warrant. If that recommendation is accepted, any person refusing to provide access information to a device or site that is the subject of a warrant would, in effect, be undermining the warrant.
- 12.178 It is instructive to compare such offending to other offences that are currently in the Act. Failing to stop a vehicle when required to do so by an officer exercising a search power is punishable by three months' imprisonment.¹⁶⁶ This offence would probably arise most often when officers are executing a warrantless power, as opposed to a search warrant. Failing to comply with a production order or an examination order is punishable by up to one year's imprisonment for

162 Issues Paper, above n 31, at [6.128]–[6.134].

163 As we noted in our Issues Paper, above n 31, at [6.132] n 83: s 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. Therefore technically the option of a fine is already available.

164 In Chapter 7 at paragraph [7.50], we recommended that a data surveillance warrant should only be available in relation to an offence punishable by up to seven years' imprisonment and certain other specified offences.

165 Section 3(1).

166 Section 177.

an individual or a fine of \$40,000 for a body corporate.¹⁶⁷ These offences involve contravention of a direct order made by an independent judicial officer.

12.179 Our view is that non-compliance with section 130, if our recommendation at paragraphs [12.39]–[12.43] above is accepted, would almost always amount to an indirect contravention of a judicial order.¹⁶⁸ We think that makes the offence more serious than failing to stop but less serious than direct contravention. Accordingly we recommend that the maximum penalty should be increased to six months' imprisonment for an individual¹⁶⁹ or a \$20,000 fine for a body corporate.¹⁷⁰

RECOMMENDATIONS

- R46 Section 130 (duty of persons with knowledge of computer system or other data storage devices or Internet site to assist with access) should be amended to clarify that the privilege against self-incrimination only protects a person from having to disclose the content of access information if the content is itself incriminating. The section should provide that an enforcement officer may require a person to provide any assistance that is reasonable and necessary to access a device or an Internet site.
- R47 The maximum penalty for non-compliance with section 130 of the Act should be increased to six months' imprisonment for an individual or a \$20,000 fine for a body corporate. This will require an amendment to section 178.

167 Sections 173 and 174.

168 The situation where it would not indirectly contravene a judicial order is where a person refuses to provide assistance in urgent circumstances where a warrantless search of the device is justified. Such cases are likely to be rare and we do not see this as having an effect on the appropriate maximum penalty. As explained by the Legislation Design and Advisory Committee, “[t]he maximum penalty should not be disproportionately severe, but should reflect the worst case of offending”: *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) ch 21, part 6.

169 The penalty of six months' imprisonment is in keeping with the Law Commission's recent recommendation concerning the appropriate penalty for committing contempt by breaching a court order: *Law Commission Reforming the Law of Contempt of Court: A Modern Statute* (NZLC R140, 2017) at 38. Appendix 1 of that Report also contains a table listing the penalties for similar offences.

170 We do not think that it is worth complicating the penalty provision by expressly including the option of a fine for an individual. As noted in n 163 above, the option is already available through s 39(1) of the Sentencing Act 2002.

Chapter 13

Warrantless powers

INTRODUCTION

- 13.1 In our Issues Paper, we identified some possible issues in relation to the existing warrantless powers in the Search and Surveillance Act 2012 (the Act). We have dealt with some of those issues elsewhere in this Report:
- In Chapter 4, we considered whether the Act should expressly limit the use of warrantless powers to situations where it is not practicable to obtain a warrant. We recommended that the Act be amended to include a general principle that a warrant or order should be obtained in preference to exercising a warrantless power.
 - In Chapter 12, we considered whether all searches of electronic devices should be conducted pursuant to a warrant. We recommended amendments to remove the ability of a person executing a warrantless search power under the Act to automatically examine an electronic device. We recommended this should be replaced by a power to seize and secure the device, pending an application for a search warrant. We also recommended a limited ability to search electronic devices without a warrant in urgent circumstances.
- 13.2 We also addressed two issues relating to warrantless powers that arose incidentally during the course of our review:
- In Chapter 12, we recommended that further consideration should be given to amending the Act (through the introduction of Internet access authorisation and remote execution authorisation regimes) to regulate how enforcement officers use the Internet to access online data from an electronic device. We also recommended that further consideration should be given to including a new warrantless power in the Act to initiate or continue an Internet search (which would be subject to a record-keeping requirement).
 - In Chapter 7, we recommended that enforcement officers should be able to conduct surveillance without a warrant to prevent offending or avert an emergency; and to locate high-risk offenders who are subject to electronic monitoring and abscond after tampering with their electronic monitoring device.
- 13.3 In this chapter, we discuss the following outstanding issues in relation to the Act's warrantless powers:
- Whether any amendments to the thresholds for exercising warrantless powers under the Act are necessary. We conclude they are not.
 - Whether the Act should be amended to provide a new power to enter a property without a warrant when an electronic monitoring device has been tampered with. We think that it should.

CURRENT LAW

- 13.4 As we explained in our Issues Paper,¹ prior to the enactment of the Search and Surveillance Act, the warrantless powers available to New Zealand Police were found in various statutes and the common law. The Act sought to codify the existence and scope of those powers. It did not seek to incorporate the powers available to regulatory agencies, which remain in separate statutes.²
- 13.5 There is a wide range of warrantless powers available to Police under the Act. The rationale for these powers is to allow Police to respond to urgent circumstances where there is an overriding public interest in the granting of such a power.³ Broadly speaking, the various public interests that justify exercising warrantless powers include:⁴ apprehending an offender who is a flight risk or who is unlawfully at large;⁵ preventing the imminent loss of or damage to evidential material;⁶ and averting an immediate risk to the life or safety of a person or serious damage to property.⁷
- 13.6 In the 2015/16 reporting year, Police exercised warrantless search powers on 7,553 occasions; and 4,328 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.⁸

THRESHOLDS FOR EXERCISING WARRANTLESS POWERS

Issues Paper

- 13.7 In our Issues Paper we asked a general question about whether the preconditions for the exercise of warrantless powers under the Act achieve their intended purpose and are realistic to apply.⁹
- 13.8 During our preliminary consultation it had been suggested to us that:¹⁰
- The powers can be difficult to apply in practice because of the wide variety of circumstances in which they can be exercised and the need for police officers to remember the various threshold requirements applicable in each case.
 - The preconditions in section 8 (which permits a police officer to enter a place or vehicle without a warrant to search for and arrest a person) can be difficult to satisfy. The officer is required to have reasonable grounds to believe that, if entry to the place or vehicle is not effected immediately, the person will leave the location to avoid arrest.¹¹ It is difficult for an officer to forecast another person's intentions.¹²

1 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [7.6] [Issues Paper].

2 See Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [53]–[54].

3 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at 22.

4 See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.90].

5 See, for example, ss 7–8 of the Search and Surveillance Act 2012.

6 See, for example, s 15.

7 See, for example, s 14.

8 New Zealand Police *Annual Report 2015/16* at 151.

9 Issues Paper, above n 1, question 31.

10 At [7.9]–[7.14].

11 Or that evidential material relating to the offence will be destroyed, concealed, altered or damaged.

12 For example, 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).

- It was also suggested to us that police officers sometimes use warrantless powers too readily, in circumstances where the threshold of “reasonable grounds to believe” is not properly met.¹³

Submissions

- 13.9 The submissions we received generally thought that the thresholds were realistic to apply and struck an appropriate balance between the interests of law enforcement and the individual.
- 13.10 We received several submissions (including from the Auckland District Law Society Inc) that were of the view that warrantless powers are sometimes too readily invoked; but did not consider this was an issue that could be addressed through amendments to the Act. For example, one submitter considered the power in section 8 is sometimes used where the requisite belief is not held, but considered the solution to this problem lay in further education and training for police officers rather than through any widening of the section 8 power.
- 13.11 We also received a comment from the District Court that warrantless powers are occasionally used too readily, but the issue is able to be adequately resolved by the courts when considering whether the exclusion of improperly obtained evidence is proportionate to the impropriety of the way it was obtained under section 30 of the Evidence Act 2006.
- 13.12 We received one submission that supported amending the section 8 preconditions to make them simpler to apply (by no longer requiring reasonable grounds to *believe* the person will leave the location to avoid arrest or will destroy evidential material).

Our view

- 13.13 In our view, if there is improper use of warrantless powers this should be addressed through further education and training for police officers rather than through any amendments to the thresholds that apply to their exercise. We also consider that the principle we recommended in Chapter 4 that recognises a preference for warrants over the use of warrantless powers will help to reinforce the exceptional nature of warrantless powers.
- 13.14 In particular, we do not consider that the difficulty in satisfying the section 8 preconditions is reason enough to justify widening the power. That power was intended to be available in a relatively small number of cases only. As the Law Commission observed in its 2007 Report, *Search and Surveillance Powers*:¹⁴

We acknowledge that in some instances the threshold we propose may be difficult for a police officer to meet and that the power may be available in only a relatively small number of cases. However, that is as it should be: a power which authorises entry by force into a dwelling-house where some of the occupants might be entirely innocent, should require a high threshold.

- 13.15 In *H v R*, the Court of Appeal also observed that the power vested by section 8 “is of an extraordinary nature” and that “[t]he text and context of s 8 leave no doubt that police officers are authorised to exercise the warrantless power of entry and search only in very narrowly defined circumstances”.¹⁵ The Court emphasised that the preconditions listed in section 8 are

13 For example, because an officer holds only reasonable grounds to *suspect* that a particular circumstance exists, rather than reasonable grounds to *believe*.

14 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [5.19].

15 *H v R* [2015] NZCA 49 at [10]. In that case, a constable had entered and searched the defendant’s property without a warrant under s 8 of the Search and Surveillance Act 2012. The constable was on notice from a colleague that the defendant may not be at the property. The constable knew that the defendant had recently travelled overseas but did not know whether he had returned. The Court considered that the possibility he had returned could not constitute an affirmative, reasonably based, belief that he was at the property when the search was effected: at [14]. It followed that the constable could not form a reasonably held belief that the defendant would leave to avoid arrest: at [17]. The search therefore was not lawfully authorised by s 8. The Court excluded the evidence obtained during the search under section 30 of the Evidence Act 2006.

conjunctive, not disjunctive;¹⁶ and that a failure to meet those carefully prescribed statutory limits would render the search a trespass.¹⁷

13.16 Accordingly, we recommend no change.

TAMPERING WITH ELECTRONIC MONITORING DEVICES

Issues Paper

- 13.17 Our Issues Paper asked submitters whether the Act should permit a police officer to enter a property to search for a person subject to electronic monitoring without a warrant where there are reasonable grounds to suspect the electronic monitoring device has been tampered with.¹⁸
- 13.18 If something unusual happens to a person's monitoring device (for example, if a person tries to remove the device, or otherwise interferes with it), the Department of Corrections will receive an alert at its monitoring centre. The monitoring team will ask a field officer and/or the relevant probation officer to locate the person and ascertain whether the interference with the device was deliberate or accidental.¹⁹ In some cases, Police may be asked to respond to the alert.
- 13.19 We were told that, if Corrections receives a tamper alert and the device is inside a private property (usually the person's detention address), an officer²⁰ will generally be sent to that address, where they will knock on the door to see if the person subject to electronic monitoring is present. If nobody comes to the door, the police officer has no ability to enter the property without a warrant to check whether the person is inside.²¹ We noted this was potentially problematic, because the officer would be unable to confirm whether a person deliberately removed their device and absconded. Without this information, Police may not know whether to commence a full-scale search for the individual in the community.²²
- 13.20 As we noted in our Issues Paper, this issue recently arose in relation to a child sex offender who removed his electronic monitoring device while subject to an extended supervision order. Police was notified that his device had been tampered with and was still inside the address but had no way of knowing whether he was still there or had fled. Since there did not appear to be any applicable warrantless power under the Act to allow entry into the property in those circumstances, a police officer was unable to immediately enter and check whether he was present.²³

16 At [11].

17 At [10].

18 Issues Paper, above n 1, question 34.

19 We understand that sometimes the device can be knocked accidentally, which will still send an alert to the monitoring centre. If a person deliberately interferes with their device, they may be arrested for failing to comply with their electronic monitoring condition: see, for example, ss 71, 73(2) and 107T of the Parole Act 2002.

20 That is, a police officer, probation officer or field officer.

21 We noted that there did not appear to be any applicable warrantless power under the Act to allow entry into the property in those circumstances. In particular, ss 7 and 8 could not be relied on because they require a police officer to have reasonable grounds to believe the person is at the property; whereas the officer is more likely to suspect that a person who has tampered with their electronic monitoring device has *left* the property. See our Issues Paper, above n 1, at [7.63]–[7.65]. We are not aware of any warrantless power of entry available to a probation officer or field officer in this situation either. We have not addressed whether there ought to be such a power, as the focus of our review is on the adequacy of the existing warrantless power provisions in subpart 2 of Part 2 of the Search and Surveillance Act (which apply to police officers only). However, we envisage that if the new warrantless power we propose below for Police is accepted, the Department of Corrections will send police officers (rather than probation or field officers) to respond to tamper alerts as necessary.

22 Issues Paper, above n 1, at [7.66].

23 This incident was noted during a 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): 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.

- 13.21 We asked submitters whether a new warrantless power to permit entry to the property was justified in those circumstances.

Submissions

- 13.22 There was strong support for the creation of a new warrantless power to allow Police to enter a property to search for a person subject to electronic monitoring in those circumstances. Submitters considered that such a power would allow Police to take swift action in the event a person absconds, such as alerting appropriate individuals as well as the wider public, and starting processes to apprehend the offender. They considered this would help to ensure public safety and maintain public confidence in the electronic monitoring system.
- 13.23 We received one submission (from the Auckland District Law Society Inc) that considered a new warrantless power was unnecessary and would carry a disproportionate risk of increased privacy intrusion when compared to the magnitude of the problem identified. That submission did, however, consider that the power could be appropriately framed by limiting its application to high-risk offenders.
- 13.24 During consultation, Police and Corrections also suggested that any warrantless power should be available only in respect of certain high-risk offenders: that is, persons subject to electronic monitoring as a condition of an extended supervision order,²⁴ or as a special condition of release under the Parole Act 2002 (on parole or at the end of a long-term sentence).²⁵ At present, there are about 160 such offenders nationwide.²⁶

Our recommendation

- 13.25 We consider that a new warrantless power is justified. There is a strong public interest in apprehending people who have tampered with their electronic monitoring device and absconded, due to the risk they present to public safety. In order to set this process in train, it is necessary for Police to be able to respond in a timely and effective manner to tamper alerts by being able to confirm that a person has in fact absconded.
- 13.26 That said, we acknowledge that warrantless powers should be exceptional and will be justified only where there is a need to meet a greater public interest. To recognise this, we agree that the power should only be available to enter a property to assist in locating high-risk offenders, namely persons subject to electronic monitoring as a condition of an extended supervision order, or as a special condition of release under the Parole Act:²⁷
- Extended supervision orders can only be made if a sentencing court is satisfied that an offender has (or has had) a pervasive pattern of serious sexual or violent offending, and is satisfied that there is a high risk the offender will commit a relevant sexual offence in the future, or a very high risk the offender will commit a relevant violent offence.²⁸ Electronic monitoring is not a standard condition of an extended supervision order: it is a special condition that can be imposed by the Parole Board.²⁹

24 Under ss 107K and 15(3)(f) of the Parole Act 2002.

25 Under s 15(3)(f) of the Parole Act 2002.

26 We were given this figure by Police at the end of March 2017.

27 For the avoidance of doubt, the power would not be available to locate people who are subject to electronic monitoring as a condition of their release from a short term of imprisonment (two years or less); as a bail condition; as a condition of a sentence of home detention, community detention, or intensive supervision; as a condition of temporary release from custody or temporary removal from prison; as a condition of working or being accommodated outside the secure perimeter; or as a condition of an intensive supervision order that is made in respect of a young person.

28 Parole Act 2002, s 107L.

29 Parole Act 2002, s 107K. See also Department of Corrections “Extended supervision” < www.corrections.govt.nz > (“[t]he highest risk people may be placed under home detention-like conditions and electronic monitoring may be imposed as a special condition”).

- As for persons who are electronically monitored as a special condition of release, we mean to refer only to those people who are released at the end of a long-term sentence (a sentence of more than two years' imprisonment)³⁰ or are released on parole.³¹ We acknowledge that the people who fall into this category are not necessarily “high risk”. However, we consider that the imposition of electronic monitoring as a special condition provides some indication that there is a heightened risk of reoffending in relation to that person.³²
- 13.27 The justification for this power is shared with the new warrantless surveillance power that we proposed in Chapter 7. There is a clear public interest, as with the power we recommend in this chapter, in the timely location of high-risk offenders who have absconded, to ensure the safety of the public. We consider it would be contrary to the public interest to require warrants to be obtained in such circumstances. We note that the wording and thresholds for exercising these two new warrantless powers should be framed—to the extent possible—in a consistent manner.
- 13.28 We recommend the Act be amended to include a new warrantless power³³ that would allow a constable to enter a property to assist in locating a high-risk person subject to electronic monitoring where the constable has:
- reasonable grounds to suspect the person has tampered with the device;
 - reasonable grounds to believe the device is in the property; and
 - reasonable grounds to believe the person is not present at the property.
- 13.29 We note, for the avoidance of doubt, that this power should permit entry onto any properties where the device is believed to be located, not just the subject person’s detention address. We also consider that the requirement for reasonable grounds to believe the person is not present at the property will be met where a constable takes reasonable steps to ascertain whether the person is at the address (for example, by knocking on the door and calling their phone number)³⁴ but is unable to make contact with anyone inside.

30 See the definition of “long-term sentence” in s 4 of the Parole Act 2002.

31 As we have noted above at n 27, we do not consider it is appropriate for the power to be available to locate people who are subject to electronic monitoring as a condition of their release from a short term of imprisonment (less than two years' imprisonment) under s 93 of the Sentencing Act 2002.

32 We also note that one of the express purposes of a special condition is to “reduce the risk of reoffending by the offender”: see s 15(2)(a) of the Parole Act 2002.

33 We consider that inserting a new stand-alone power into the Act is simpler than (as was suggested to us by two submitters) amending the definition of “unlawfully at large” in s 3 of the Act to include a person who is subject to electronic monitoring and whom a constable has reasonable grounds to suspect has tampered with their monitoring device; and permitting s 7 of the Act to then be invoked (which would also require that section to be amended to require the constable to have reasonable grounds to believe that the electronic monitoring device is there, and to have reasonable grounds to believe that the person is not present at the property). (The current definition of “unlawfully at large” already covers the situation where a person has tampered with their electronic monitoring device, but only where electronic monitoring was imposed as a condition of temporary release from custody or temporary removal from prison under ss 63 and 64 of the Corrections Act 2004, or as a condition of work or accommodation outside the secure perimeter under s 65A.)

34 The Supreme Court confirmed in *Tararo v R* [2010] NZSC 157, [2012] 1 NZLR 145 that there is an implied licence under the common law for anyone (including police officers) to enter upon, but not into, private premises for the purpose of speaking to its occupants. Within such a licence, someone entering the property is not a trespasser.

RECOMMENDATION

R48 A new provision should be inserted into Part 2 of the Act to create a warrantless power, which would allow a constable to enter a property to assist in locating a person subject to electronic monitoring as a condition of an extended supervision order or as a special condition of release under the Parole Act 2002 where the constable has reasonable grounds to:

- (a) suspect the person has tampered with the device;
- (b) believe the device is in the property; and
- (c) believe the person is not present at the property.

Chapter 14

Production orders

INTRODUCTION

- 14.1 When the Search and Surveillance Act 2012 (the Act) came into force in 2012 it introduced a new production order regime. The regime provides a streamlined process for obtaining documents that constitute evidential material in an investigation. It was envisaged that, in particular, production orders would provide a more efficient way of obtaining customer-specific business records (“customer records”) from service providers such as banks and telecommunications network operators (“telcos”).¹
- 14.2 As we explained in our Issues Paper, the main difficulty with the production order regime is that it is not always clear when it should be used.² There is overlap with the search warrant and interception regimes in the Act. There is also overlap with the information privacy principles in the Privacy Act 1993, which regulate the disclosure of personal information. The matter is further complicated by the existence of inter-related but substantively different production powers in other legislation. Since multiple techniques are available to obtain the same documentary evidence, the exact nature and purpose of the production order regime is not transparent.
- 14.3 This chapter begins with an overview of the production order regime and a discussion of the intended relationship in the Act between production orders, search warrants and surveillance warrants. We also discuss production powers in other legislation and the intersecting disclosure regime under the Privacy Act. These discussions highlight the current areas of uncertainty.
- 14.4 We then examine whether the situation would be improved if there was greater guidance as to when a production order should be obtained. We conclude that it would and explain why we think that a policy statement is the most appropriate vehicle for providing that guidance and for addressing other related issues raised by submitters. This leads to a discussion about the notification and reporting requirements that should apply in respect of production orders. We recommend that new notification requirements should be included in the Act and that the Ministry of Justice should do further work to identify the costs of implementing additional reporting requirements.
- 14.5 At the end of the chapter we look at whether there is a need to introduce a data preservation regime. A preservation notice or order would require the recipient to preserve documents pending the execution of a production order. We recommend that the Act should include such a regime as it would be particularly useful in the context of international investigations. Finally, we comment on the availability of production orders issued in respect of foreign service providers.

1 In this Report, we use the term “service provider” to refer to private sector businesses that provide a service to customers. This includes telecommunications network operators, internet service providers, banks, electricity and gas suppliers and transport companies.

2 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [9.23]–[9.39] [Issues Paper].

THE PRODUCTION ORDER REGIME IN THE ACT

- 14.6 The Act treats documents as a special category of evidential material. If an enforcement officer wishes to search for and seize documents during the course of an investigation, that officer may be able to apply for a production order.³ The Act only enables such an application if the officer independently has a power to apply for a search warrant in respect of the documents.⁴ Put simply, where documents are involved, the Act provides an enforcement officer with the option of applying for a production order instead of a search warrant.
- 14.7 A production order is made in respect of a person⁵ rather than a place, vehicle or other thing.⁶ It requires the person to provide specified documents that are in their possession or control to a particular enforcement officer.⁷ It is an offence for the person to refuse to comply with the order without reasonable excuse.⁸
- 14.8 An issuing officer may make a production order if there are reasonable grounds:⁹
- to suspect that an offence has been, is being, or will be committed; and
 - to believe that the documents sought:
 - constitute evidential material in respect of the offence; and
 - are in, or will come into, the possession or control of the person against whom the order is sought.

These conditions are essentially the same as those required to obtain a search warrant in respect of documents under section 6 of the Act.¹⁰

- 14.9 A production order must specify when and how the person is to produce the documents.¹¹ This includes a direction as to whether the documents are to be produced on one occasion or on an ongoing basis.¹² An order can remain in force for up to 30 days.¹³ This means that a production order under the Act may be forward-looking. It may relate to documents that do not exist at the time of the order but that “come into the possession or under the control” of the person named in the order while it is in force.¹⁴ The phrasing in the Act is passive. This means that, while a production order may be forward-looking, it cannot require a person to create documents that would not otherwise have existed.¹⁵

The intended relationship to search warrants

- 14.10 It is evident from the wording of the Act and its legislative history that production orders were primarily introduced to provide a less-intrusive alternative to search warrants.

3 “Enforcement officer” is defined in s 3 of the Search and Surveillance Act 2012 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.

4 Section 71(1).

5 Section 74.

6 Section 6.

7 Section 75(1)(a).

8 Section 174(1).

9 Section 72.

10 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.24]. This point was also made by the majority in *R v A* [2017] NZSC 42 at [18].

11 Section 75(2)(e).

12 Section 75(2)(d).

13 Section 76.

14 Sections 71(g) and 75(1)(b).

15 This conclusion is reinforced by the definition of “document” in s 70 of the Act. This definition includes call associated data and the content of telecommunications, as long as that data and content is stored by a network operator “in the normal course of its business”.

14.11 Prior to the Act coming into force, it was common practice for enforcement officers to execute search warrants in respect of customer records by simply informing the relevant service provider that a warrant had been obtained. That service provider would then co-operate by locating and handing over the documents. In its 2007 Report, *Search and Surveillance Powers*, the Law Commission concluded that it would be better to formalise this process in a new production order regime. This new regime would:¹⁶

- more transparently reflect the nature of the transaction;
- avoid any confusion as to how the usual execution and post-execution search warrant procedures should apply;
- avoid an enforcement officer having to specify the exact whereabouts of any document;
- be less intrusive, especially in the case of a co-operative third party; and
- be more effective.

14.12 The Law Commission specifically addressed whether there should be a lower threshold for production orders. In doing so, it considered a threshold of “reasonable grounds to suspect that the information sought will assist in the investigation of the offence”.¹⁷ The Commission decided against this approach and advised:¹⁸

... as production orders should, in our view, be available as an alternative to search warrants, attaching a lower threshold to the issue of production orders could be seen as sanctioning fishing expeditions for certain types of information when there is no compelling reason to do this.

14.13 The Law Commission also expressly considered whether, instead of production orders, production notices should be available.¹⁹ Production notices are issued by a person within an enforcement agency instead of an independent issuing officer.²⁰ The Commission rejected this option as well. It concluded that there was no justification for departing from the ordinary warrant principle requiring prior independent authorisation.²¹ It also noted that, in practice, it would be highly desirable for an issuing officer to oversee the process particularly where issues of privilege, client confidentiality or the impact on third parties may need to be considered.²² The Act reflects the Law Commission’s reasoning on these points.²³

16 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.22].

17 At [10.26].

18 At [10.26].

19 At [10.36]–[10.51].

20 “Enforcement agency” is defined in s 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.

21 At [10.46].

22 At [10.46].

23 This is evident from the Select Committee report on the Search and Surveillance Bill 2009, which relevantly states: “We think it important to note that there has been some misunderstanding about the nature of the production order regime. It was intended that production orders would provide a less intrusive alternative to a search warrant in circumstances where the party subject to the order is willing to co-operate with enforcement officers. For example, if Police needed to obtain bank records during the investigation of a crime then it would be less disruptive to the bank if it could retrieve the documents itself, rather than having police officers come in and search through its records. The regime also codifies existing case law, with the courts having previously ruled that a search warrant can be executed by Police sending the warrant to the party concerned and that party identifying and producing the relevant documents without police officers physically conducting the search”: Search and Surveillance Bill 2009 (45-2) (select committee report) at 11. See also the discussion of the legislative history of production orders in *R v A* [2017] NZSC 42 at [18]–[19].

The intended relationship to surveillance warrants

- 14.14 There is one aspect of the production order regime, however, that is different from the regime governing search warrants: production orders can be issued on an ongoing basis and can relate to documents that do not yet exist.²⁴
- 14.15 Forward-looking production orders were included in the Act as a response to the Law Commission's original recommendation that there should be a monitoring order regime of general application in New Zealand.²⁵ A monitoring order and a forward-looking production order are, in essence, the same thing.
- 14.16 At the time of the Commission's 2007 Report, there were two types of monitoring orders available in New Zealand:
- A monitoring order under the Proceeds of Crime Act 1991 (now repealed). This enabled a High Court judge to require a financial institution to provide transaction information in respect of a specified person to New Zealand Police on an ongoing basis for up to three months. The order could only be made in the context of proceeds believed to be derived from drug dealing offending.²⁶
 - A call data warrant under the Telecommunications (Residual Provisions Act) 1987 (now repealed). This enabled a District Court judge to require a telco to supply call associated data in respect of a specified person to Police or the New Zealand Customs Service on an ongoing basis for up to 30 days. Call associated data did not include the content of calls or text messages.²⁷
- 14.17 In its 2007 Report, the Commission identified several cases where the existing search warrant, call data warrant and monitoring order processes were ineffective in obtaining relevant customer records from banks and telcos.²⁸ It highlighted text messages as a particular area of concern because often enforcement agencies would need to obtain both a search warrant and a call data warrant in order to get both the information about, and the content of, the messages.²⁹ The Commission considered that it would be more transparent and effective if all of this information could be obtained through a wider monitoring order process.³⁰
- 14.18 Both the Law Commission, and later the Select Committee when it considered the Search and Surveillance Bill, recognised that there was potential for overlap between monitoring orders and surveillance device warrants. The Law Commission commented:³¹

A common feature of monitoring orders and surveillance device warrants is that they authorise enforcement officers to gather evidential material on an ongoing basis. There is, however, one important difference. A surveillance device warrant authorises an enforcement officer to capture or

24 Sections 103(4)(h) and (j) of the Act state that, if it is expressly authorised, a search warrant may be executed on multiple occasions over a period of up to 30 days. The Act is drafted, however, in a way that makes it clear this is the exception rather than the rule. It is also not clear whether the warrant could relate to a document that was not in existence at the time of the application. The doubt is caused because the application must describe the items "believed to be in" a particular location (s 98(1)(e)). This is in the present tense. The Law Commission clearly considered that a search warrant could not be used to achieve the same result as a monitoring order (which, in effect, is a forward-looking production order as we discuss at paragraph [14.15]). After describing the nature of monitoring orders in the Commission's 2007 Report it observed at [10.61]: "Existing warrant procedures are deficient in providing a mechanism to obtain such information [that is, records of financial transactions on an ongoing basis] and they could not be readily adapted to do so".

25 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) recommendations 10.12–10.17.

26 Proceeds of Crime Act 1991, ss 77-81A (now repealed).

27 Telecommunications (Residual Provisions) Act 1987, ss 10A to 10S (now repealed).

28 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.68]–[10.70].

29 At [10.75]–[10.76].

30 At [10.76].

31 At [10.63].

record information as it is occurring, in real time. In contrast a monitoring order is concerned with the recovery of information after it has been stored or otherwise held.

- 14.19 By the time the Select Committee considered the Bill, monitoring orders had been re-framed as forward-looking production orders. In relation to these orders, telcos expressed concern that “[enforcement] agencies could use production orders as a means of intercepting data so as to bypass the protections in the surveillance device regime”.³² The Committee recommended amendments to the provisions in the Bill to clarify that a production order would not require a person or organisation to produce a document that it would not ordinarily keep. It stressed that “production orders are intended to cover only information already stored, and not to authorise interception”.³³
- 14.20 As we discuss further below, the availability of forward-looking production orders raises two problems:
- it complicates the relationship between production orders and search warrants, which colours the discussion as to whether the same rules around notification should apply; and
 - in relation to text messages, it creates uncertainty as to when a production order should be used and when an interception warrant is required.

PRODUCTION POWERS IN OTHER LEGISLATION

- 14.21 There are numerous other statutory provisions in New Zealand that can be used to compel the production of documents in criminal or regulatory investigations. Most of these provisions were enacted primarily for regulatory purposes, but many have an incidental law enforcement component. The table below outlines a few pertinent examples. These are general production powers: in other words, they are not limited in terms of what documents can be compelled or who can be compelled to produce them.³⁴

PRODUCTION POWERS IN OTHER LEGISLATION				
Agency	Statutory provisions	Notice or order	Requirements	Associated examination power
<i>New Zealand Customs Service</i>	Section 161 Customs and Excise Act 1996: further powers in relation to documents ³⁵	Notice from within the agency	The chief executive must consider that the documents are necessary or relevant to an investigation under the Act.	Yes – the person may also be required to appear before a specified Customs officer and answer all questions put to the person concerning the documents.
<i>Serious Fraud Office</i>	Section 5 Serious Fraud Office Act 1990: power to require production of documents	Notice from within the agency	The Director must have reason to believe that the documents may be relevant to any suspected case of serious or complex fraud.	Yes – the person may also be required to answer questions with respect to the whereabouts or existence of any further documents that may be relevant to the investigation.

³² Search and Surveillance Bill 2009 (45-2) (select committee report) at 12.

³³ At 13.

³⁴ As an example of a more specific power, s 201 of the Fisheries Act 1996 empowers a fisheries officer to require the production of “any permit, authority, approval, permission, licence, or certificate issued in respect of any vessel or person”.

³⁵ See also s 160 of the Customs and Excise Act 1996, which enables the chief executive to issue a notice in respect of specified documents if there are reasonable grounds to suspect that a specified offence has been committed. The provision relates to goods that have been, or are likely to be, dealt with unlawfully or that have been seized.

PRODUCTION POWERS IN OTHER LEGISLATION				
<i>Inland Revenue</i>	Section 17 Tax Administration Act 1994: information to be furnished on request of Commissioner	Notice from within the agency	The Commissioner must consider that production of the documents is necessary or relevant for any purpose relating to the administration or enforcement of any of the Inland Revenue Acts.	Potentially – the person may also be required to “furnish any information in a manner acceptable to the Commissioner”.
<i>Ministry of Social Development</i>	Section 11 Social Security Act 1964: power to obtain information	Notice from within the agency	The chief executive can issue a notice requiring the production of documents for a variety of purposes including determining whether a person is, or was, entitled to receive a particular benefit or payment under the Act.	Potentially – a person may also be required to provide the department with “such information as the chief executive requires”.
<i>Ministry of Business, Innovation and Employment and New Zealand Customs Service</i>	Sections 134Y and 155E Trade Marks Act 2002: judge may order documents to be produced	Order issued by a judge	The judge must be satisfied that there are reasonable grounds to believe that a person is in possession or control of documents that are evidence of, or may be of significant relevance to the investigation of, an offence against the Act.	No
	Sections 134Y and 144D Copyright Act 1994: judge may order documents to be produced	Order issued by a judge	The judge must be satisfied that there are reasonable grounds to believe that a person is in possession or control of documents that are evidence of, or may be of significant relevance to the investigation of a specified offence against the Act.	No
<i>New Zealand Police</i>	Section 105 Criminal Proceeds (Recovery) Act 2009: production order	Order issued by a judge	The judge must consider that the Commissioner has reason to believe that a person has possession or control of documents that are relevant to an investigation by the Commissioner under the Act or to any proceedings under the Act.	No

14.22 The most significant observation to make about these production powers is that they are predicated on different and in most cases less onerous requirements than the production order regime in the Search and Surveillance Act:

- The majority of the powers in the table can be exercised without obtaining prior independent approval from an issuing officer.
- There is no statutory requirement to show that there are “reasonable grounds to suspect” that an offence has been committed, although there must be an investigation into particular offending.
- Most of the powers in the table can be invoked in relation to documents that “are relevant” or “may be of significant relevance” to the investigation. In comparison, the Search and Surveillance Act requires that the documents must “constitute evidential material” in respect of the relevant offence.³⁶

14.23 Further, some of the production powers in the table are associated with a power to require the relevant person to answer questions about the documents they have produced. Again, this is markedly different from the production order regime in the Act. That regime relates solely to documents. If an enforcement officer wishes to require a person to produce documents and answer questions about them under the Search and Surveillance Act, the examination order regime would need to be used.³⁷ That regime carries much higher statutory thresholds and can only be used by Police.³⁸

³⁶ Given the broad definition of “evidential material” in s 3 of the Search and Surveillance Act, this last requirement may, in effect, be the same but there is room for doubt. In that regard, see the approach the Law Commission took to the possibility of “lowering the threshold” for production orders as described in paragraph [14.12].

³⁷ Subpart 12 of the Act.

³⁸ Sections 34 and 36.

- 14.24 In light of these observations, it is important to clarify that the recommendations in this chapter only relate to the production order regime under the Search and Surveillance Act. Production powers in other legislation are fundamentally different.
- 14.25 As we explained in Chapter 2, regulatory powers of search and seizure are often wider than law enforcement powers and there may be sound policy reasons for that.³⁹ We acknowledge that the production powers in the Serious Fraud Office Act 1990 are not regulatory in nature. However, as the Law Commission observed in 2007, those powers were “introduced in light of international experience at the time, which suggested that traditional investigative powers had been found wanting” in combating serious and complex fraud.⁴⁰ It is not within the scope of our review to revisit those policy decisions.
- 14.26 We do, however, acknowledge that the existence of these overlapping production powers can be a source of frustration for enforcement agencies. Regulatory agencies may have access to two or more very different production powers and the distinctions as to when each is available may seem arbitrary. For Police, most of the powers in the table are not available at all. This can seem counter-intuitive and ineffective when police officers are investigating similar offending to other enforcement agencies or conducting joint investigations.⁴¹ This commonly occurs in relation to drug and fraud offending. However, Police has access to other extensive law enforcement powers, including warrantless powers that may be available where there is a strong public interest in documents being obtained immediately.⁴²
- 14.27 Our view is that the existence of production powers in other legislation should not have an impact on the production order regime in the Act. It is plain from the legislative history that an express decision was made to reject the option of modelling the regime in the Act on those powers.⁴³ That reasoning remains sound today.

DISCLOSURE OF DOCUMENTS UNDER THE PRIVACY ACT 1993

- 14.28 Up until very recently, there was considerable doubt as to the relationship between the Privacy Act and the production order regime in the Act. We discussed this issue at length in our Issues Paper, and it was the main driver behind our question: “Should the Act be clearer about when a production order should be required?”⁴⁴
- 14.29 The problem arises because the Search and Surveillance Act does not require an enforcement officer to obtain a production order in any given situation – it simply permits it.⁴⁵ Therefore, if an enforcement officer wishes to obtain documents from a person during the course of an investigation, the officer could simply ask for the documents in the same way that any ordinary citizen could.⁴⁶ No express statutory authority is required.

39 Chapter 2 at paragraphs [2.76]–[2.78].

40 See Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.46] (“[t]he production notice power enacted in the Serious Fraud Office Act 1990 was part of a package of ‘forceful and rigorous powers to combat serious and complex fraud’ that were introduced in light of international experience at the time, which suggested that traditional investigative powers had been found wanting”) and at [10.48].

41 See *P v R* [2016] NZCA 153 where the Court of Appeal commented that, even in the context of a joint investigation, Customs cannot invoke its requisition power in s 161 of the Customs and Excise Act 1996, under Police direction. Instead, Customs officers must obtain and to some degree inspect the documents before relying on the power in s 175D of the Act to pass the documents on to Police.

42 This point was made by the Select Committee in response to a submission by Police that production orders should be made more readily available: Search and Surveillance Bill 2009 (45-2) (select committee report) at 12. It is also worth noting that information privacy principle 11(f) in s 6 of the Privacy Act 1993 enables agencies to release personal information to Police voluntarily if there is a risk to public safety or to an individual’s life or safety.

43 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.26], [10.47] and [10.48].

44 Issues Paper, above n 2, at [9.9]–[9.59].

45 Search and Surveillance Act 2012, s 71.

46 For further discussion, see paragraphs [4.19]–[4.22] in Chapter 4, which explain the “third source” of authority for State actors.

- 14.30 In such a situation, however, the holder of the documents may not be able to lawfully comply with the request. That is because the information privacy principles in the Privacy Act contain a general prohibition on an “agency” voluntarily disclosing “personal information” to a third party.⁴⁷
- 14.31 Personal information is defined broadly in the Privacy Act as meaning “information about an identifiable individual”.⁴⁸ “Agency” is also defined broadly to mean “any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector”.⁴⁹ As a result of these definitions, the prohibition is widely applicable.
- 14.32 There are, however, numerous exceptions to the prohibition. For example, it does not apply if the disclosure is to the individual concerned or if that individual consents.⁵⁰ Further, non-compliance is permissible if disclosure is necessary to lessen or prevent a serious threat to public safety or to the life or health of an individual.⁵¹ Most relevant for our purposes is the exception in principle 11(e)(i), which states that non-compliance is permissible where disclosure:⁵²
- ... 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.
- 14.33 In light of this exception (and putting to one side the production powers in other legislation), enforcement officers seeking documentary evidence have two options: ask the person or company in control of the documents to provide them voluntarily or obtain a production order. Neither the Privacy Act nor the Search and Surveillance Act expressly identifies the factors that enforcement officers should consider in making this decision. The Acts also do not clearly set out what factors a requested person or service provider should take into account in deciding whether to voluntarily disclose any documents or whether to insist on a production order. As a result, inconsistent practices have developed.
- 14.34 Since we published our Issues Paper, the Supreme Court has released its decision in a pre-trial appeal, *R v A*, which directly addresses this point.⁵³ The majority judgment⁵⁴ contains a framework for how enforcement officers and requested persons and service providers should address these issues. We adopt this framework and set out the majority’s rationale below.

R v A

- 14.35 Early on in the investigation into the alleged offending in *R v A*, Police approached three electricity service providers and asked them to provide copies of power bills associated with two of the respondent’s properties. The service providers voluntarily complied with the requests, and the information gleaned from the power bills was then used to obtain a subsequent production order (for mobile phone data) and search warrants (in respect of the two properties). One of the issues the Supreme Court considered was whether the power bills had been obtained in breach of the New Zealand Bill of Rights Act 1990 (NZBORA) and/or the Privacy Act.
- 14.36 For the majority the decisive issue was whether the power bills had been obtained as a result of an “unreasonable search” contrary to section 21 of NZBORA.⁵⁵ To determine this question

47 Privacy Act 1993, s 6, principle 11.

48 Section 2.

49 Section 2.

50 Section 6, principles 11(c) and 11(d).

51 Section 6, principle 11(f).

52 Section 6, principle 11(e).

53 *R v A* [2017] NZSC 42.

54 Delivered by Arnold J, on behalf of himself, William Young, Glazebrook and O’Regan JJ.

55 At [17] and [47].

the majority first considered whether there was a “search” and applied the test of whether the information gathering activity invaded a “reasonable expectation of privacy”⁵⁶ in accordance with the approach of Blanchard J in *Hamed v R*.⁵⁷

- 14.37 In deciding to apply this test, the majority expressly rejected the Court of Appeal’s view in *R v R* that, if information is obtained consistently with the privacy principles, there can be no “search” for the purposes of NZBORA.⁵⁸ We agree with this conclusion. Whether or not an enforcement officer has conducted a “search” for documents cannot be determined solely on the basis that the person in control of the documents was entitled to hand them over and did so voluntarily. Such an approach would be inconsistent with the fact that the Search and Surveillance Act regulates consent searches.⁵⁹
- 14.38 The majority in *R v A* explained that the “reasonable expectation of privacy” test is directed at protecting “a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state”⁶⁰ and includes information “which tends to reveal intimate details of the lifestyle and personal choices of the individual”.⁶¹
- 14.39 In applying the test to the facts of the case, the majority considered the following factors:
- **The nature of the information at issue** – the majority considered that the monthly aggregate power bills did not reveal intimate details about the respondent, but commented that a more particularised power bill could.⁶²
 - **The circumstances in which the information was obtained** – the majority noted that the electricity service providers owned the data, collected it for commercial reasons, and supplied it without the need for an intrusive search of any property. Further, the service providers had a direct interest in supplying the information to law enforcement because the offending under investigation could well have included the theft of electricity, as it is commonplace for large-scale drug operations to tap into a power line or bypass the electricity meter.⁶³
 - **The nature of the relationship between the parties** – the majority considered the three contracts containing the terms of supply and observed that each stated that personal information would be held in accordance with the Privacy Act and referred to the possibility of disclosure. However, the majority placed very little weight on this observation. It commented that arguments could be made both ways as to what was implied by the contracts. Further, it advised that such standard form contracts should be assessed with caution given the wide variety of information that is generated in customer relationships.⁶⁴

56 At [50].

57 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 205 at [163] and following. In *Lorigan v R*, the Court of Appeal noted that it was not entirely clear whether there was majority support for Blanchard J’s approach in the other *Hamed* judgments. However, the Court concluded that the test of “state intrusion into reasonable expectations of privacy” was broadly consistent with the *Hamed* judgments and should be applied: *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22].

58 *R v A* [2017] NZSC 42 at [64] and *R v R* [2015] NZCA 165 at [63]. The majority further stated (at [38]) that whether information is obtained consistently with, or in breach of, the Privacy Act may be relevant to whether it was improperly obtained in terms of s 30 of the Evidence Act 2006, but is not determinative, because the privacy principles do not create rights that are enforceable through the courts.

59 Part 4, subpart 2 of the Search and Surveillance Act 2012.

60 *R v A* [2017] NZSC 42 at [63] relying on *R v Plant* [1993] 3 SCR 281 (which is also discussed at [55]–[57]).

61 At [63].

62 At [66].

63 At [67].

64 At [68]–[71].

- 14.40 The majority concluded that the respondent had no reasonable expectation of privacy in the power bills.⁶⁵ Police therefore had not obtained those documents in breach of NZBORA because there was no search. The majority further observed that in circumstances of exigency a search (in the form of voluntary provision of documents) may not be unreasonable. But where there is time to obtain a production order or search warrant, the search may well be unreasonable.⁶⁶
- 14.41 By contrast, Elias CJ in her minority judgment considered that this issue turned on the Privacy Act.⁶⁷ The Chief Justice concluded that the power bills had been obtained in breach of that Act, primarily because Police did not explain to the electricity companies why voluntary disclosure under the exception (as opposed to compelled production under a production order) was “necessary” to avoid prejudice to an investigation or prosecution.⁶⁸ Urgency was highlighted as an obvious example of the type of situation where this requirement might be fulfilled.⁶⁹ The Chief Justice commented that if there were simply insufficient grounds to apply for a production order, the requirement would not be fulfilled.⁷⁰
- 14.42 The judgments in *R v A* indicate that an enforcement agency trying to decide between requesting voluntary disclosure and applying for a production order should consider:⁷¹
- whether there are exigent circumstances, such as urgency, which may justify voluntary disclosure; and
 - if not, whether a person (other than the requested person) has a reasonable expectation of privacy in the documents. If the answer is yes, the request will amount to a search, and a production order should generally be obtained to avoid the risk of breaching NZBORA.
- 14.43 Our view is that the majority judgment in *R v A* has removed some, but not all, of the doubt surrounding the issue of when a production order should be obtained. As we explain below, there is residual uncertainty as to how to apply the reasonable expectation of privacy test in practice. There are also other areas of uncertainty.

A STATUTORY REQUIREMENT TO OBTAIN A PRODUCTION ORDER

- 14.44 In our Issues Paper, we asked whether the Act should be amended to require enforcement officers to obtain a production order in certain situations.⁷² We put forward three possible options.⁷³ A production order could be required:
- when the documents engage a reasonable expectation of privacy;
 - when the documents contain specified information and/or are held by specified service providers (for example, telcos, internet service providers, banks, electricity and gas suppliers, and transport companies); or

65 At [72].

66 At [64].

67 At [119]–[123].

68 At [178]–[179].

69 At [159].

70 At [180], [184] and [191].

71 The majority and the Chief Justice agreed that exigent circumstances are highly relevant (see the majority at [64] and the minority at [159]). They also agreed that the privacy interest in the requested document is also relevant. As discussed in this chapter, the majority adopted the “reasonable expectation of privacy” test (see [73](d)) but the Chief Justice went further and indicated that a production order should be obtained if the document contains personal information and there were no exigent circumstances indicating that voluntary disclosure was “necessary” to avoid prejudice to the investigation and no other justification for disclosure under the Privacy Act 1993 (at [159]).

72 Issues Paper, above n 2, question 41.

73 At [9.51]–[9.59].

- when the criteria for a production order are met and one could be obtained without prejudicing the investigation.

Submissions

- 14.45 We received 20 submissions on this question. We note that the Supreme Court's decision in *R v A* was delivered after we received submissions.
- 14.46 Submitters were fairly evenly divided as to whether a statutory requirement is desirable. The majority (who were mainly service providers) favoured greater clarification in the Act. The minority (who were mainly enforcement agencies) opposed such an amendment. However, none of the three options we proposed for the statutory amendment found much favour with submitters. Only two submitters expressed clear support for any of the options, both of whom preferred the second option or a variation on it.
- 14.47 The New Zealand Telecommunications Forum Inc suggested a variation involving a two-step process. First, a production order should be required to obtain customer records from certain service providers, such as telcos. Second, where documents are going to be sought from any other person or entity, the enforcement agency should consider whether there is a reasonable expectation of privacy in the document.
- 14.48 Significantly, the question in our Issues Paper prompted several submitters to comment more broadly on:
- the impact that the increasing use of technology is having in this area;
 - the breadth of requests for voluntary disclosure and production orders; and
 - the distinction between forward-looking production orders and interception warrants.

The impact of technology

- 14.49 As presented in the submissions, the crux of this problem is as follows. Society's growing reliance on technology is creating an abundance of reliable, real evidence that is of high value to enforcement agencies. That evidence often takes the form of customer records held by banks and telcos. In the past, service providers often disclosed information from these records to enforcement agencies on a voluntary basis in reliance on the exception in privacy principle 11(e).
- 14.50 Over the last five years, however, as the use of technology has dramatically risen, so has the number of law enforcement requests for customer records. As well as requests for voluntary disclosure, production orders and other production powers are increasingly being used. Large service providers are now in the position of having to employ staff whose sole responsibility is to respond to enforcement agency requests and production orders. The New Zealand Telecommunications Forum Inc advised us that in the telco industry there has been approximately a 15 per cent increase in the number of production orders in the last three years and the cost of processing the orders has increased by 32 per cent (due to the increasing size and complexity of each order). Over the same period requests for voluntary disclosure of personal information went up by approximately 34 per cent and the processing cost went up by 15 per cent. This has dramatically increased the compliance costs for service providers.
- 14.51 We were advised that, at the same time, customers are becoming more and more concerned about the privacy of their personal information. The growing public concern has increased the reputational risk associated with providing information voluntarily to law enforcement rather

than by compulsion. There are also legal risks associated with voluntary disclosure, as service providers owe obligations of confidentiality to their clients.

- 14.52 The result of these trends is that service providers have started to push back on requests for voluntary disclosure and are more frequently insisting on production orders. This is becoming problematic for enforcement agencies, as voluntary disclosure can be essential at the early stage of an investigation, to collect sufficient information to obtain production orders and search warrants. Without it, investigations may not progress.

The breadth of production orders

- 14.53 Many of the submissions that we received expressed concern about the breadth of requests for voluntary disclosure and production orders. We were advised by a telco that a single request or order may relate to hundreds of phone numbers and may require all of the call information associated with those numbers. Another service provider suggested that in such cases it is better to receive a request for voluntary disclosure than a production order, as the breadth of the search can be negotiated.
- 14.54 One legal practitioner commented that production order applications tend to be more generalised than search warrant applications. As an example, he referred to cell phone data. He explained that there is a tendency to simply assert that because an individual is suspected of committing a particular type of offending (for instance drug dealing), their text message and call data is likely to constitute evidential material. This may be enough to obtain a production order.⁷⁴ However, greater specificity is required to obtain a search warrant. It would not be sufficient to simply link the individual to an address and state that drug dealers often keep money and drugs at their houses. He concluded that there may be a need to amend the statutory test for production orders, given the clear privacy interests in communications data.

Forward-looking production orders

- 14.55 Some service providers asked in their submissions for greater clarity around the difference between forward-looking production orders and interception warrants.
- 14.56 One telco explained that forward-looking production orders are often used to obtain the content of text messages or location data from cell phones in near to real time (up to every 15 minutes). It commented that in practice this achieves the same outcome as interception and circumvents the surveillance warrant regimes in the Act. It asked for clarification as to whether this is permissible and commented that—from a technical perspective—it would be more efficient in most of these cases to use its specialised interception technology.

Our view

- 14.57 We are conscious that there are several recent developments that may already address some of the problems submitters identified. As we have explained, the majority decision in *R v A* provides new judicial guidance on when a production order is required. The Privacy Commissioner will publish guidance in 2017 on how agencies⁷⁵ should apply the law enforcement exception in principle 11(e) when considering requests for voluntary disclosure. Police recently updated its Information Request Form to make it clear that providing

74 This issue was discussed in *F v Police* [2017] NZHC 992 at [36]: “I agree ... that the police may use text messages regularly in investigations but this is only able to be done where the relevant statutory criteria are met. If this could be assumed without being expressly stated, then police would be able to obtain text message data in relation to almost any suspect with minimal explanation being given, on the basis that simply because people communicate with one another via cell phones and text messages, the contents of their cell phones can be expected to contain evidence of any alleged criminal offending that they have engaged in”.

75 As discussed at [14.31], “agency” is defined broadly in s 2 of the Privacy Act 1993 to mean “any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector”.

- information in response to the Form is voluntary. This is a standard form that police officers use to request a person or a company to provide information on a voluntary basis. Police has also entered into Letters of Agreement with various large service providers that relate to these issues.
- 14.58 We are also conscious that we have no current reference to review any aspect of the Privacy Act. In those circumstances, we consider that our reform objectives are to support the current initiatives, to clarify the nature of the production order regime and to encourage the provision of information on a voluntary basis where it is appropriate to do so.
- 14.59 The last objective reflects the fact that we agree with the conclusion of the majority of the Supreme Court in *R v A* that non-sensitive personal information (by which we mean personal information that does not engage a reasonable expectation of privacy) can be disclosed by a service provider to an enforcement agency without a production order, if that is necessary to progress an investigation.⁷⁶ For example, this might include the fact that a person is a customer of a bank or a telco. Without that information an enforcement officer could never obtain a production order in respect of that person's bank or phone records.
- 14.60 We consider that our three goals could be achieved by:
- providing greater clarity for enforcement agencies, the private sector and the public in general on when production orders should be used (as opposed to requests for voluntary disclosure or surveillance warrants);
 - taking steps to address the legitimate concerns raised by service providers in relation to escalating costs and reputational and legal risk; and
 - promoting targeted searching under the production order regime.
- 14.61 In our view, none of our goals would be advanced by amending the Act to make production orders mandatory in certain situations. In Chapter 4, we outlined the reasons why a statutory rule based on the reasonable expectation of privacy test would not provide clarity and consistency.⁷⁷ In short, that test requires a highly nuanced assessment and there is scope for reasonable minds to disagree. Accordingly, it would not work as a mandatory statutory rule.
- 14.62 Amending the Act to state expressly that a production order must be obtained in respect of certain types of service providers and/or certain types of documents would create a more workable test. However, we think that it would also create artificial distinctions and would not stand the test of time as a statutory test. Both the service industry and the diversity of forms of data are rapidly changing.
- 14.63 Finally, we do not think the situation would be much clearer if the Act simply required enforcement officers to apply for a production order whenever they have sufficient grounds to do so. That would not reflect the level of privacy intrusion involved and would not resolve the issue of whether voluntary disclosure is ever appropriate. As we have explained, we think that voluntary disclosure of certain information is essential for effective law enforcement.
- 14.64 Instead we consider that our reform objectives would be significantly advanced by amending the Act to include a requirement that a policy statement must be issued in respect of Search and Surveillance Act production orders.

⁷⁶ *R v A* [2017] NZSC 42 at [64].

⁷⁷ Chapter 4 at paragraphs [4.16]–[4.24].

A PRODUCTION ORDER POLICY STATEMENT

- 14.65 We introduced the general concept of policy statements in Chapter 5. There we explained that policy statements are designed to provide greater guidance for enforcement agencies in “grey areas”, including where there is any doubt as to whether an activity may be lawful or reasonable in light of the case law surrounding section 21 of NZBORA. We noted that policy statements would promote consistency, transparency and accountability in these areas. That is because they would be issued and regularly reviewed by the chief executives of enforcement agencies, would be publicly available and would need to be taken into account by any enforcement officer undertaking the specified activity.
- 14.66 The policy statements that we have recommended elsewhere in this Report generally relate to investigative activities that are not regulated by statute or are only regulated by statute in part. That is where the issues of uncertainty arise. Production orders are different. Production orders are regulated by sections 70–79 of the Act and we do not think that the policy statements should have any wider application. However, as we have outlined in this chapter, the existence of multiple overlapping investigatory techniques has created considerable uncertainty as to when to apply for a production order and what that application should contain. It would be better for enforcement agencies, service providers and the public in general if there was one readily accessible document setting out the relevant considerations.
- 14.67 In that regard, we think it would be helpful if enforcement agencies jointly issued a policy statement in respect of Search and Surveillance Act production orders or if the Commissioner of Police issued a model policy statement that other enforcement agencies could adjust on an as-needed basis.
- 14.68 We think that the policy statement should contain:
- examples of the types of documents that do, and do not, engage a reasonable expectation of privacy;
 - advice on how to frame production order applications in respect of certain types of documents in a manner that minimises intrusions on privacy; and
 - guidance on when it is appropriate to obtain a production order, as opposed to a surveillance warrant.

Reasonable expectation of privacy examples

- 14.69 Under *R v A* the primary consideration for an enforcement officer deciding whether or not it is prudent to apply for a production order is whether the relevant documents engage a reasonable expectation of privacy. As we indicated above we consider that this is the right test – but we do not think that it should take the form of a mandatory statutory rule. There is a need for greater flexibility.
- 14.70 To promote consistency and transparency in how this test is applied, we think that a policy statement should explain the approach that enforcement agencies intend to take by setting out various examples. In accordance with *R v A* the examples would need to consider the nature of the information in issue, the circumstances in which it was obtained and the general nature of the relationship between the parties. In practice, however, the nature of the information will be the most important consideration. That is because most of the time the customer–service

provider relationship will be fairly similar and, as the Supreme Court has indicated, the exact contractual terms between the parties should not ordinarily be given much weight.⁷⁸

- 14.71 The examples could be drawn from case law and could also be based on analogies, likely scenarios and any relevant content from the Letters of Agreement between Police and service providers. They could then be adjusted as more case law is generated.⁷⁹ Over time this should create a clearer picture for enforcement agencies, and, importantly, for service providers and the public, as to the appropriate way of dealing with different types of documents.
- 14.72 This greater consistency and transparency will in turn assist in alleviating some of the legal and reputational risk associated with the voluntary disclosure of personal information. The public would be reassured that service providers are only disclosing non-sensitive personal information in this way and could see from the examples exactly what types of information that would be.

Minimising intrusions on privacy

- 14.73 As explained above, submitters expressed concern that production orders often require service providers to produce large volumes of customer-related data, to allow enforcement officers to search for much more limited evidential material. This raises similar issues to those discussed in Chapter 12, as to whether too much irrelevant material is seen during digital searches.
- 14.74 As noted in Chapter 12, this problem would be addressed, in part, by our recommendation in Chapter 4 that the Act should include a principle “that powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected”. However, we consider that context-specific guidance in a policy statement would also be beneficial.
- 14.75 We envisage that this guidance could be drafted along similar lines as the guidance on production orders recently issued by the Ontario Superior Court in *R v Rogers Communications Inc.*⁸⁰
- 14.76 In that case two telcos applied for a declaration that various inter-related production orders were overly broad and unconstitutional. The production orders related to data from more than 37 cell phone towers and in respect of approximately 41,000 subscribers. Police requested the data to assist in determining who was likely to have been present at the location of a series of robberies. In light of their previous experiences with overly broad production orders, the telcos asked the Court to issue guidance on how applications for production orders in respect of cell phone tower data should be framed.
- 14.77 The Court declared that the orders authorised unreasonable searches and breached section 8 of the Canadian Charter of Rights and Freedoms 1982.⁸¹ In terms of guidance it advised that Police should include the following information in production order applications:⁸²

78 *R v A* [2017] NZSC 42 at [68].

79 Some examples can already be drawn from the majority decision in *R v A* [2017] NZSC 42. For example, it can be inferred that there is no reasonable expectation of privacy in aggregate power bills or in the fact that a person is a customer of a particular service provider. The majority also indicated that a person might have a reasonable expectation of privacy in a more detailed power bill and commented (in fn 96): “[s]ome types of smart meter may collect power consumption data in a way that does reveal intimate details of a person’s lifestyle and other choices”. We are also aware of currently unresolved litigation concerning whether there is a reasonable expectation of privacy in customer contact details, bank statements and travel records.

80 *R v Rogers Communications Inc* 2016 ONSC 70 at [65] and [66]. Police participated in developing the guidelines by identifying general principles and instructions that would help to ensure that Police applied for effective and “privacy enhanced” tower dump production orders (at [17]).

81 Section 8 of the Canadian Charter of Rights and Freedoms 1982 provides that “[e]veryone has the right to be secure against unreasonable search and seizure”.

82 *R v Rogers Communications Inc* 2016 ONSC 70 at [65] and [66].

- a statement or explanation that demonstrates the officer seeking the order is aware of the principles of incrementalism and minimal intrusion⁸³ and has tailored the request with that in mind;
- an explanation as to why all of the named locations or cell towers, and all of the requested dates and time parameters, are relevant to the investigation;
- an explanation as to why all of the types of records sought are relevant;
- any other details or parameters that might permit the target of the production order to conduct a narrower search and produce fewer records;
- a request for a report based on specified data instead of a request for the underlying data itself (or if the underlying data is required, there should be a justification for that request);⁸⁴ and
- confirmation that the types and amounts of data that are requested can be meaningfully reviewed by enforcement officers.

14.78 For completeness, we note that some guidance could also be gleaned from the New Zealand Court of Appeal's decision in *M v R*.⁸⁵ In that case Police obtained a production order in respect of the text messages sent from and received by two cell phone numbers over a 15-day period. The 15-day period included the day of the burglary that was under investigation. Police considered that the text messages would also contain evidence of other burglary offending, although no particular suspected additional offences were identified in the application. The Court concluded that, on the facts of the case, a production order should only have been issued in relation to the day of the suspected offending or for a maximum of four days. The 15-day period was considered to be "well outside the range of a reasonable period" so as to be in breach of section 21 of NZBORA.⁸⁶

14.79 We consider that guidance in this area will improve the production order regime by minimising intrusions on privacy and may have the incidental benefit of reducing the compliance costs for service providers.

The relationship to surveillance warrants

14.80 As explained in Chapter 9, we do not consider that it is problematic for an enforcement officer to apply for a production order to obtain cell phone data that effectively enables the officer to track a person.⁸⁷ The tracking device warrant regime is based on the same statutory threshold as production orders. Interception, however, is different.

83 These principles stem from s 8 of the the Canadian Charter of Rights and Freedoms 1982 and were described by the Court in *R v Rogers Communications Inc* 2016 ONSC 70 at [63] as "fundamental principles". To describe the principle of minimal intrusion, the Court at [41] quoted the following passage from Gerald Chan "*Morelli* and Beyond: Thinking about Constitutional Standards for Computer Searches" (2012) 33(2) For the Defence - The Criminal Lawyers' Association Newsletter: "The animating policy is that the state must always be alive to the privacy interests of the individual and must always infringe such interests as little as possible". The Court stated at [54] that an incremental approach is supported by the principle of minimal intrusion. This requires a minimally intrusive data set to be obtained in the first instance to support the particular stage of the investigation and then an enforcement agency can seek incrementally broader production orders as necessary. See Tim Banks "Dragnet No More? Recent guidance on production orders" (18 January 2016) Privacy and Cybersecurity Law < www.privacyandcybersecuritylaw.com/dragnet-no-more-recent-guidance-on-production-orders > .

84 In relation to this requirement a Canadian commentator has observed that "[t]he idea that a report, rather than raw data, should be the norm may not be popular with all recipients of production orders. This could be potentially onerous in itself and, in some cases, may place recipients of these production orders in the position of performing investigative work on behalf of the police": Banks, above n 83. We agree with this observation and note that there is no case law in New Zealand that suggests that such a report should be the norm.

85 *M v R* [2015] NZCA 101.

86 At [47]. The Court of Appeal went on to conduct the balancing exercise required under s 30 of the Evidence Act 2006. The Court concluded, at [60], that the evidence obtained pursuant to the production order was not admissible at the appellants' trial.

87 Chapter 9 at paragraphs [9.73]–[9.74].

- 14.81 Only limited enforcement agencies can apply for an interception warrant, and such warrants are only available in investigations into offending that carries at least a seven-year maximum penalty, or certain other specified offences.⁸⁸ Production orders, like search warrants, are generally available in respect of any imprisonable offence.⁸⁹
- 14.82 As noted by submitters, this distinction is problematic where a forward-looking production order can be obtained to enable an enforcement officer to receive text messaging data in near to real time. Even though it is less intuitive, this is also a problem in relation to ordinary production orders. Any production order in respect of text messages can be used to obtain the same information as an interception warrant.
- 14.83 We consider that a policy statement could usefully provide guidance for enforcement agencies, service providers and the public as to when it is reasonable to obtain a production order as opposed to an interception warrant. The policy statement should explain that there are four notable differences between forward-looking production orders and interception warrants:
- Interception is an inherently indiscriminate process. It is not possible for an enforcement officer executing an interception warrant to stop and start the interception process to avoid listening to or viewing irrelevant material. By contrast, it is possible for an enforcement officer to obtain incremental production orders. That is, an officer could obtain an initial production order covering a short period of time. If the documents produced then indicated that further documents would be relevant, the officer could obtain a second production order for a longer time period.
 - Interception warrants can be issued for up to 60 days, whereas production orders can only last for 30 days.⁹⁰
 - Interception warrants can be issued in respect of oral or written communications and are often used to obtain communications made by suspects.⁹¹ Production orders can similarly capture communications made by suspects but are limited to written communications. During the passage of the Search and Surveillance Bill, the Select Committee recommended raising the threshold for obtaining interception warrants. This was largely because it was concerned about the level of privacy intrusion involved in “audio surveillance”.⁹² We consider that there is a slightly lower expectation of privacy in written communications, such as text messages, as the individual is more likely to be aware of the possibility of the message being forwarded or shown to another person.
 - The target of an interception warrant is not ordinarily notified of the interception, whereas (as we explain further below) we recommend that the target of a production order should be notified, even if that notification is routinely postponed.
- 14.84 In light of those differences, we suggest that the policy statement should state that production orders in respect of text messages should only cover the shortest period of time that is reasonable in the circumstances, bearing in mind that a second production order is a possibility. This guidance will need to be framed in a way that is practical and realistic for law enforcement.

88 Search and Surveillance Act 2012, ss 45, 49(5) and 50.

89 Sections 6 and 71.

90 Sections 55(1)(c) and 76.

91 In their submission, the New Zealand Law Society argued that one of the reasons why the threshold for interception should not be lowered was because interception often targets communications made by suspects. See paragraph [8.17] in Chapter 8.

92 Search and Surveillance Bill 2009 (45–2) (select committee report) at 4: “some forms of surveillance have more effect on privacy than others and should be treated accordingly. It is our view that audio surveillance and the use of visual surveillance devices in circumstances that require enforcement officers to enter private property are intrusions upon privacy which should be authorised only for the investigation of the most serious offending”.

14.85 *M v R* provides an example of how we see this approach working in practice. In that case only the text messages sent within four days of the alleged burglary were of interest in tracing the movements of the suspect, the stolen goods and/or in identifying co-offenders. If Police discovered evidence of other offending when reviewing those messages, then an officer could have applied for a second production order covering a longer time period. The example illustrates why it is important to justify the length of time covered by the production order in order to ensure that it is “reasonable”. Such an approach accords with our principle of minimal intrusion and the jurisprudence surrounding general warrants, which indicates that production orders should be as specific as the circumstances allow.⁹³

RECOMMENDATION

- R49 A provision should be inserted into the Act requiring a policy statement to be issued in respect of production orders. That statement should contain guidance on how to:
- (a) apply the reasonable expectation of privacy test described in the majority judgment in *R v A* [2017] NZSC 42;
 - (b) prepare appropriately tailored production order applications; and
 - (c) decide whether to apply for a production order or an interception warrant in any given case.

THE FINANCIAL COST OF PRODUCTION ORDERS

- 14.86 During our consultation, service providers reiterated the concerns raised in their submissions about the rising compliance costs associated with production orders. In doing so, they asked us to consider whether the Act should be amended to include a cost recovery or cost contribution regime in relation to production orders. There is precedent for this in the Telecommunications (Interception Capability and Security) Act 2013. That Act states that a law enforcement agency “must pay for the actual and reasonable costs” incurred by a service provider in providing assistance to enable the execution of a surveillance warrant.⁹⁴
- 14.87 We discussed this proposal with several enforcement agencies and legal stakeholders. It received mixed feedback. There was a general consensus that a cost recovery regime would be unworkable in relation to production orders, as thousands are made each year. A cost recovery regime would be beyond the means of many enforcement agencies and might prevent Police from investigating lower-level offending. It was also noted that there is a moral and social duty on all citizens to co-operate with law enforcement and that assistance is not usually reimbursed.⁹⁵
- 14.88 On the other hand, many of the people we consulted accepted that service providers are now disproportionately carrying the burden of assisting law enforcement. Further, some of that assistance is being provided on a voluntary basis. There is a need to maintain good working relationships and to ensure that costs do not become prohibitive. It was noted that the

⁹³ For a discussion of that jurisprudence, see Chapter 12 at paragraphs [12.44]–[12.55].

⁹⁴ Section 115 of the Telecommunications (Interception Capability and Security) Act 2013.

⁹⁵ See *Rice v Connolly* [1966] 2 QB 414 at 419 (“every citizen has a moral duty or, if you like, a social duty to assist the police”) and *Moulton v Police* [1980] 1 NZLR 443 (CA) at 444. In *R v A* [2017] NZSC 42 the Chief Justice commented at [181]: “As indicated I consider that some of the statements in some of the cases about the freedom of an agency holding personal information to act as a ‘good corporate citizen’ in responding to requests by law enforcement agencies (for example *R v Cox* (2004) 21 CRNZ 1 (CA) at [66]) need reassessment in light of the policies of the Privacy Act and the availability of orders under the Search and Surveillance Act with its policy of balancing law enforcement interests with human rights and rights of privacy”.

introduction of a cost contribution regime might have the incidental effect of encouraging more targeted production orders. We were also advised that the cost of assistance disproportionately affects small businesses and could limit their access to the market.

- 14.89 Our preliminary view is that a cost contribution scheme may be justified. We do not think that service providers should simply pass these costs on to customers. Such an approach would not promote transparency and could unduly limit competition. There is an uncomfortable tension that needs to be squarely confronted. Service providers and enforcement agencies need to work co-operatively together and by necessity that may require sharing costs. However, there is a need to ensure that this is not perceived to be a money-making venture. A transparent cost contribution scheme could potentially include a threshold for eligibility or a cap on the contribution in order to keep the cost to enforcement agencies down.
- 14.90 We do not, however, recommend that the Search and Surveillance Act be amended to include such a scheme. This issue is not confined to the Search and Surveillance Act. Although we do not know exact figures, there is evidence to suggest that service providers are responding to even greater numbers of requests from enforcement agencies that are made under other legislation (namely, voluntary disclosure in accordance with the Privacy Act and the production powers described in the table at paragraph [14.21] above).⁹⁶ If a cost contribution scheme related only to production orders, there is a risk that it would simply incentivise the use of alternative investigative techniques.
- 14.91 To develop a broadly applicable and workable cost contribution scheme it would be necessary to analyse detailed data concerning all of the relevant costs and to consult widely with affected enforcement agencies and service providers. It would also be necessary to address the underlying philosophical question of how much of law enforcement's costs should be borne by the private sector. It was not within the scope of our terms of reference to undertake these tasks during the course of this review. We do, however, think that it would be beneficial for this work to be undertaken in the future.

RECOMMENDATION

- R50 The Ministry of Justice should undertake further work to identify and evaluate the options for establishing a cost contribution scheme in respect of:
- (a) production orders and notices obtained by enforcement officers and directed to service providers; and
 - (b) requests from enforcement officers for service providers to supply customer records on a voluntary basis.

NOTIFICATION

- 14.92 The Search and Surveillance Act contains detailed rules regarding notification and search warrants. Before entering a place, an enforcement officer executing a search warrant must announce their intention to search and must provide the occupier of the place with a copy of the warrant.⁹⁷ At the end of the search (or if that is not possible, within seven days), the officer must also provide the occupier with an inventory of everything seized pursuant to the warrant.⁹⁸

96 Privacy Commissioner *Transparency Reporting Trial August–October 2015: Full Report* (2016) at 28.

97 Search and Surveillance Act 2012, s 131(a) and (b).

98 Section 133.

If no occupier is present at the time of the search, the officer must leave a written notice, a copy of the warrant and an inventory (if available) in a prominent place before leaving.⁹⁹

- 14.93 These rules do not apply to production orders. That is because a production order is directly addressed to the person who is in possession or control of the documents that are sought. That person is the equivalent of an occupier in the search warrant context. There is, however, a significant difference. The occupier of a place that is being searched may well be the suspect who is under investigation or an associate of that person. By contrast, the recipient of a production order will often be a service provider and the suspect is likely to be one of their customers. Our understanding is that service providers do not tend to notify their customers of production orders. That is partly because enforcement agencies routinely advise against such notification, because of the impact that it may have on the ongoing investigation.
- 14.94 In our Issues Paper, we asked whether the Act should be amended to enable or require a person whose personal information is sought under a production order to be notified of that fact.¹⁰⁰ If not, we asked whether the Act should expressly prohibit the recipient of a production order from informing the relevant person.¹⁰¹ We received mixed responses to these questions.

Submissions

- 14.95 The majority of submitters (who were mainly enforcement agencies) opposed notification. They advised that, in practice, production orders are used differently to search warrants. They are generally obtained very early on in investigations and often provide the basis for subsequent search and surveillance warrant applications. A notification requirement would therefore significantly impede ongoing investigations. Enforcement agencies did not consider that having an option to defer notification would adequately address this problem. The grounds for deferral would be made out in such a high percentage of cases that applying for deferral would become an academic exercise.
- 14.96 Submitters also drew comparisons to other investigative techniques that may involve obtaining personal information from a third party. This includes search warrants, production powers in other legislation and voluntary disclosure in accordance with the Privacy Act. None of the regimes governing these techniques requires a person to be notified if an enforcement officer obtains their personal information. Submitters queried why the position in relation to production orders should be any different. They noted that there is independent scrutiny of production orders by issuing officers, so there is already more privacy protection than there is in respect of some of the other techniques.
- 14.97 For similar reasons, the majority of submitters also favoured the option of amending the Act to prohibit a recipient of a production order from notifying any person whose personal information is sought. Several considered this to be a matter of clarification rather than a change in policy.
- 14.98 The New Zealand Telecommunications Forum Inc advised that, in its view, notification is already prohibited by law. It referred to express prohibitions in other legislation containing production powers and to the Telecommunications Privacy Code, which it has interpreted as requiring telcos to act in a manner that does not prejudice ongoing investigations. Police commented that section 179 of the Search and Surveillance Act is potentially broad enough to charge a person in receipt of a production order with an offence, if they notified the person

⁹⁹ Section 131(4).

¹⁰⁰ Issues Paper, above n 2, question 43.

¹⁰¹ Question 44.

whose personal information is sought.¹⁰² Other submitters did not express a clear view on what the law is, or what it should be on this point. Instead, they simply stated that the Act should clearly identify what the recipient of a production order ought to do in this situation.

- 14.99 Those who opposed any restrictions being placed on notification did so mainly on principle. They suggested that production orders should operate in the same way as search warrants. The Search and Surveillance Act does not prevent an occupier from notifying any other person of the existence of a search warrant; therefore the recipient of a production order should not be so constrained. These submitters contended that the concerns around the impact on ongoing investigations could be met by allowing for notification to be postponed, just like notification of a search warrant can be deferred. They argued that routinely deferred notification is better than no notification at all.

Our view

- 14.100 One of the main reasons why the occupier of a place must be notified when a search warrant is executed is to promote accountability.¹⁰³ This is done by ensuring that a person affected by the search has sufficient details of the intrusion to seek further information if necessary, or to challenge the issue of the warrant.¹⁰⁴ We do not think that the production order regime, as it currently stands, provides that accountability.
- 14.101 Without consulting their customer, a service provider is unlikely to have sufficient knowledge about the circumstances of a case to hold an enforcement agency to account for the exercise of their search power. Arguably, it is also not their place to mount this challenge as it is the customer, not the service provider, who has the real privacy interest in the documents at issue. In practice, however, the customer will only become aware of the production order if charges are laid and its existence comes to light during the disclosure process. That will not happen in every case.
- 14.102 In our view, it is important—as a matter of principle—that production orders are subject to the same level of accountability as search warrants. As explained earlier in this chapter, production orders provide an alternative to search warrants. Forward-looking production orders are slightly different, but the threshold for obtaining one is the same and there is no compelling reason why these orders should be subject to a different level of accountability. We acknowledge that there is no requirement to notify the target of an interception warrant but, as we discussed

102 Section 179 of the Search and Surveillance Act makes it an offence to disclose information acquired through search or surveillance. Section 179(1) states that “[n]o person who, as a consequence of any thing specified in subsection 2 [that is, the exercise of a search or surveillance power, an examination order, a production order or an activity specified in a declaratory order], 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 performance of that person’s duties, functions or powers”. The offence is punishable in the case of an individual to a term of imprisonment not exceeding six months, and in the case of a body corporate, to a fine not exceeding \$100,000.

103 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [6.131].

104 At [6.131].

above at paragraphs [14.81]–[14.83], interception is conceptually different and is subject to a much higher statutory threshold.¹⁰⁵

- 14.103 It also needs to be kept in mind that production orders and search warrants are evidence-gathering techniques. They are not intelligence-gathering techniques. They can only be executed to locate documents or items that “constitute evidential material” in relation to a specific offence. That makes them different to some production powers in other legislation and to voluntary disclosure under the Privacy Act. Furthermore, as explained above, most of the production powers in other legislation are regulatory in nature and voluntary disclosure should be limited to non-sensitive personal information or to urgent situations. Different rules regarding notification are appropriate in those circumstances.
- 14.104 Despite these observations, it is entirely legitimate for enforcement agencies to use production orders very early on in investigations provided the statutory criteria are met. Customer records will often contain reliable and clear evidence of a suspect’s movements, communications and/or financial transactions. The fact that this information is held by a third party makes it easier for enforcement officers to obtain the information without alerting the suspect straight away. This is a logical starting point. We simply think that the person whose information is obtained should be notified of the privacy intrusion at an appropriate time, to promote accountability. We think that the appropriate time is immediately after the production order has been complied with, unless there are case-specific reasons to justify postponing notification.
- 14.105 In terms of who should be notified, we acknowledge that there is a dilemma. A production order may relate to documents that contain personal information in respect of a vast number of people. For example, a bank statement or a printout of text messages may contain personal information about both parties to each transaction or message. It would be impracticable for an enforcement officer to notify every person whose personal information is affected. Accordingly, we propose that an enforcement officer should only be required to take reasonable steps to notify the “target” or “targets” of a production order. By this we mean any person whose personal information is the primary or central focus of a production order. In practice, this would usually mean the one customer whose records are sought. That person may well be identified by name in the order.
- 14.106 In terms of postponement, we think that similar rules should apply as those that exist in relation to search warrants. At the time of applying for the production order the enforcement officer should specify whether compliance with the usual notification requirements would “endanger the safety of any person” or “prejudice an ongoing investigation”.¹⁰⁶ If the issuing officer is satisfied that non-compliance is required for one of those reasons, they should be able to

105 The Law Commission originally recommended that the targets of surveillance should be notified after the fact: Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) recommendation 11.21. A cabinet paper prepared in response to the Report explains why this recommendation was not accepted: Cabinet Business Committee “Law Commission Report on Search and Surveillance Powers: Paper 1: Overview” (14 March 2008) CBC (08) 84 at [67]–[75]. The paper records: “Customs believes that the oversight of Parliament is the appropriate method to ensure poor practice is rectified rather than notification and is very concerned that any notification to the subject of surveillance will prejudice maintenance of the law. It is common for individual suspects to be of ongoing interest to law enforcement agencies; disclosing the fact of surveillance makes it much more difficult to surveil that individual or their associates again in future. Customs maintains that notification has the potential to expose the precise nature of the techniques and technologies employed by law enforcement agencies, and may also lead to the identification of undercover law enforcement officers and members of the public who assist them through allowing their premises to be used for surveillance purposes. Customs also believes that overseas law enforcement agencies will be unlikely to work cooperatively with New Zealand agencies if there is the potential that the NZ agency may have to notify an individual thus jeopardising an international operation and revealing techniques also utilised by those overseas agencies”. In light of these concerns and a general concern raised by Police, it was proposed to Cabinet that it would be preferable for an enforcement agency to report back to the issuing officer after executing a surveillance warrant. As part of that report back process the issuing officer could order that the target should be notified “if satisfied that the warrant should not have been issued or that there has been a serious breach of its terms or that the use of the device was significantly outside the scope permitted by the emergency warrantless power and that, having regard to the gravity of the breach, the public interest in notification outweighs any potential prejudice to on-going or subsequent investigations or to the safety of informants or undercover officers” (at [69]). That approach is reflected in ss 59–61 of the Search and Surveillance Act.

106 Search and Surveillance Act 2012, s134(1).

- postpone notification for up to 12 months.¹⁰⁷ If, at the end of that period, the original rationale for postponement continues to exist, a further postponement of (or dispensation from) the notice requirement should be possible.¹⁰⁸
- 14.107 Significantly, we think that if notification is postponed then the production order should expressly prohibit the recipient from notifying the target until after the postponement period has expired.¹⁰⁹ In this way the production order would clearly set out the recipient's obligations. It would make it plain that notification by the recipient is prohibited. Notification in those circumstances would amount to non-compliance with the production order. That is an offence under the Act and is punishable by up to one year's imprisonment in the case of an individual and a fine of up to \$40,000 in the case of a body corporate.¹¹⁰
- 14.108 We consider that such an approach is more appropriate than amending section 179 of the Act to enable prosecution under that provision. As we explained in our Issues Paper, section 179 is directed towards enforcement officers and those who assist them in executing a search power.¹¹¹ It is an offence for such persons to disclose any personal information that they obtain as a result of executing the search power. This offence is designed to protect privacy, not the integrity of ongoing investigations. In addition, it would be odd to treat the recipient of a production order as being akin to a person assisting in the execution of that order.
- 14.109 Finally, we note that the same problem we have identified above in respect of production orders could theoretically arise in relation to a search warrant. It is easy to imagine that a search warrant could be issued to obtain a suspect's personal information, but the suspect may not be the occupier who is present at the place when the warrant is executed. A flat-sharing scenario is the obvious example. Theoretically, an occupier could choose not to tell their flatmate that a search warrant was executed and that their bedroom was searched. The flatmate could therefore be unaware of the intrusion and unable to challenge it.
- 14.110 Accordingly, we recommend that the Act should also be amended to require an enforcement officer to take reasonable steps to ensure that any person whose personal information is the main focus of a search warrant is notified as soon as practicable after the warrant is executed. We do not envisage that it would be particularly onerous for enforcement agencies to meet this requirement. Ordinarily the occupier will at least be an associate of the suspect and can either contact them directly or provide their contact details to the enforcement agency.

107 Section 134(3).

108 Section 135. We note that, as in the case of a search warrant, if an enforcement officer did not comply with any notification provision in respect of a production order, there would be a significant risk that the courts would find that the order was executed in breach of s 21 of the New Zealand Bill of Rights Act 1990 and any evidence obtained as a result of the order could be potentially inadmissible at trial under s 30 of the Evidence Act 2006.

109 An enforcement officer may obtain a further postponement or dispensation from the notification requirements after the production order has been issued. Therefore the Act should state that an enforcement officer must notify the recipient of the order of any variation to the postponement period.

110 Section 174.

111 Issues Paper, above n 2, at [9.73]–[9.77].

RECOMMENDATION

- R51 The Act should be amended to include new notification requirements in respect of production orders and search warrants. The amendments should include the following:
- (a) Inserting a provision into the Act to require an enforcement officer to take reasonable steps to notify the target(s) of a production order or a search warrant as soon as possible after the order or warrant has been executed. By “target”, we mean any person whose personal information is a primary or central focus of a production order or search warrant.
 - (b) Inserting a provision into the Act enabling an issuing officer to defer compliance with the notification obligations in respect of a production order for up to 12 months if the notification would endanger the safety of any person or prejudice an ongoing investigation. A second postponement of up to 12 months or a dispensation from compliance should also be available.
 - (c) Amending section 75(2) (which explains what a production order must set out) to state that a production order must set out any period during which compliance with the notification obligation in respect of a production order has been deferred.
 - (d) Amending section 75(1) (which explains what a production order requires the recipient to do) to require the person against whom a production order is made not to disclose the existence of that order to any person who is a target of the order until after any period of deferred notification has expired.

REPORTING

- 14.111 The Search and Surveillance Act requires enforcement agencies to include in their annual reports:¹¹²
- the number of occasions on which a warrantless power of search or surveillance under the Act was used and the number of persons charged where the investigation was significantly assisted by the exercise of such a power;
 - the number of applications that were granted or refused for a surveillance warrant, an examination order or a declaratory order (where the agency can make such applications) and the number of persons charged where the investigation was significantly assisted by the execution of such a warrant or order; and
 - additional specified information in respect of surveillance warrants and declaratory orders.
- 14.112 The Act does not, however, contain any reporting requirements in respect of production orders or search warrants.
- 14.113 The Law Commission’s original rationale for this approach was that the administrative burden associated with reporting could only be justified in respect of warrantless powers, on the basis that they are not the subject of any other external scrutiny; and surveillance warrants, on the basis that they are almost always executed covertly.¹¹³ In those situations it was considered desirable to bolster accountability and transparency through annual reporting.¹¹⁴ The

¹¹² Search and Surveillance Act 2012, ss 171 and 172.

¹¹³ Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [15.46]–[15.48].

¹¹⁴ At [15.44]–[15.46].

Commission treated residual warrants (which later became declaratory orders) as being similar to surveillance warrants in this regard.¹¹⁵ The Select Committee then recommended adding reporting requirements for examination orders to recognise the fact that these orders were “one of the most contentious aspects of the [B]ill” and that therefore “stringent judicial and parliamentary oversight” was required to reassure the public about their use.¹¹⁶

14.114 As we explained in our Issues Paper, there has been a trend in recent years towards increased transparency reporting by service providers both overseas and in New Zealand.¹¹⁷ These reports provide statistics on the number and nature of requests that enforcement agencies make to providers each year for customer records. This trend is attributable to the increasing interest that customers are showing in the privacy of their personal information, and in knowing how and when this information is accessed by law enforcement.

14.115 We asked whether, in light of this trend, the Act should be amended to require enforcement agencies to report on the number of production order applications granted or refused each year.¹¹⁸

Submissions

14.116 Of the 12 submissions that directly responded to this question, seven favoured the reporting requirement and five opposed it. All of the submissions engaged in some kind of cost-benefit analysis, although there was considerable variation in their assessment of both the costs and the benefits.

14.117 In relation to costs, enforcement agencies advised that they do not currently collect such statistics and that installing new infrastructure to do so would be expensive. By contrast, others suggested that production orders already go through a formal issuing process in court, so recording the application and whether it was successful should not create a significant additional burden. It was accepted, however, that given the volume of production orders (and search warrants) that are issued each year and the fact that production orders tend to be used early on in investigations, it would be unworkable to also require reporting on whether their execution substantially assisted in charges being laid.

14.118 In relation to benefits, enforcement agencies and others we consulted questioned whether there would be any tangible value in reporting. They commented that, without reporting obligations attaching to similar regimes (that is, production powers in other legislation, voluntary disclosure and search warrants), the bare numbers of production orders would present an incomplete picture and could not usefully inform policy. A broader evaluative exercise would be necessary for that. On the other hand, those who favoured increased reporting suggested that it would be an appropriate response to the public’s increased interest in the exercise of search powers. Reporting would provide the public with insight into the workings of law enforcement and would enhance the public’s trust that search powers are being used responsibly.

14.119 Submitters on both sides of this debate drew the comparison to search warrants and proposed that there should be no distinction between search warrants and production orders for reporting purposes. If a reporting requirement was solely introduced in respect of production orders, search warrants would be the only investigative technique in the Act that would not be the subject of annual reporting.

115 At [15.47].

116 Search and Surveillance Bill 2009 (45-2) (select committee report) at 8 and 10.

117 Issues Paper, above n 2, at [9.67] and [9.68].

118 Issues Paper, above n 2, question 42.

Our view

- 14.120 In our opinion there is potential for reporting to have considerable benefits. There are intangible benefits in the form of increased transparency, accountability and trust. There are also tangible benefits in that reporting provides evidence of current practice. That evidence is directly relevant to discussions about resourcing and reform.
- 14.121 These are generic benefits and we accept that there is always an administrative cost to be incurred to realise them. Nonetheless, three of the observations that we have made about production orders in this chapter suggest that the cost of reporting may be justified.
- 14.122 First, as we explained in paragraph [14.93], the person whose personal information is targeted under a production order is not usually notified of that fact. Even if our recommendation for notification is accepted, it may be necessary for notification to be routinely deferred. Therefore, like surveillance warrants, it appears that production orders tend to be executed covertly in the sense that the person whose privacy interest is intruded upon is generally not aware of that fact. As such, additional accountability could be viewed as necessary.
- 14.123 Second, as we noted in paragraph [14.91], there is a policy need to obtain statistics on how many production orders are processed by service providers each year (along with information about voluntary disclosure and the use of production powers in other legislation). This information is needed to work out whether a cost contribution scheme is required and if so, how that scheme should best be structured. If this information is already being collected, the additional burden of reporting would be lessened.
- 14.124 Third, there is increased public interest in how service providers protect the privacy of their customers and how they respond to requests for personal information from law enforcement. If increased transparency in the private sector is not mirrored by increased transparency in government, this could needlessly damage public trust.
- 14.125 However, we do not consider that we are in possession of sufficient information at this stage to make a firm recommendation that the Act should be amended to include a reporting requirement in respect of production orders. That is because we do not yet have a clear understanding of the costs that would be involved in setting up the necessary systems to enable this to occur. The courts do collect information on the number of production orders made and approved per year, but there are gaps in that data and there are issues of categorisation.
- 14.126 In addition, we agree with those who submitted that reporting on the use of search warrants, other production powers and voluntary disclosure could also be justified. It is not within the scope of our terms of reference to propose reporting requirements in other legislation. Therefore, we simply recommend that further work should be undertaken to determine the costs involved in implementing a reporting requirement for production orders and search warrants. It may also be worth considering the costs involved in reporting on the use of other production powers and voluntary disclosure as well. We suggest that any further work should take into consideration the work the Office of the Privacy Commissioner is currently undertaking in respect of transparency reporting more generally, following on from its 2015 Transparency Reporting Trial.

RECOMMENDATION

- R52 The Ministry of Justice should conduct further work to identify the costs of implementing a requirement for enforcement agencies to report on the number of applications for production orders and search warrants that are granted or refused each year.

A DATA PRESERVATION REGIME

- 14.127 As noted at the start of this chapter, production orders are only available in respect of documents. The word “document” is not exhaustively defined by the Act, but includes “call associated data and the content of telecommunications” that “the network operator has storage capability for and stores in the normal course of its business”.¹¹⁹ It is clear that this covers electronic customer records that exist independently from any actions taken by law enforcement. Notably, such records usually contain personal information and under the Privacy Act they must be destroyed when there is no longer a business reason to retain them.¹²⁰
- 14.128 The ease and regularity with which customer records are destroyed poses a problem for effective law enforcement. An enforcement officer may become aware of the relevance of a customer record at around the same time as it is due to be destroyed. At present there is no ability for the enforcement officer to require the service provider to preserve that record while a production order is obtained. The enforcement officer’s only options are to request voluntary preservation and/or to try and obtain a production order as fast as possible.
- 14.129 In our Issues Paper, we explained that it is common for overseas jurisdictions to have a statutory regime that allows for the temporary preservation of data, pending the determination of an application for a production order or a search warrant.¹²¹ These regimes involve an enforcement agency either internally issuing a preservation notice, or applying to a court for a preservation order and then serving the notice or order on the service provider. Given that New Zealand does not have such a regime we asked:¹²²
- whether there is a problem with data being unavailable by the time enforcement agencies have obtained a search warrant or production order; and
 - whether the Act should be amended to include a preservation regime.

The difference between data preservation and data retention

- 14.130 The submissions we received in response to these questions illustrated that there is a fine line between data *preservation* and data *retention*. This is, however, a very important distinction.
- 14.131 Data preservation is case-specific. The data in question must be clearly identified in any notice or order and must be relevant to a specific investigation or proceeding. A preservation regime is therefore only helpful if an enforcement agency becomes aware of the relevance of data to a specific case between the time it is created and the time when it would ordinarily be destroyed. It is therefore most useful where data is only stored by a service provider for a short period of time.
- 14.132 One submitter identified mobile Internet Protocol (IP) addresses as a type of record that is often unavailable by the time an enforcement officer obtains a production order. An IP address is a unique identifier that is assigned to an electronic device by a network operator. These can be static (that is, fixed or permanent) or dynamic. If an IP address is dynamic, the record identifying the device and linking it to a particular user of a network may only exist for a short window of time. Some service providers hold this information for business purposes for less than seven days, while some do not retain this information at all. Given that this is information

119 Search and Surveillance Act 2012, s 70.

120 Privacy Act 1993, s 6, principle 9.

121 Issues Paper, above n 2, at [9.83] and [9.94]–[9.97].

122 Questions 45 and 46.

that can be quickly identified as critical to an investigation and is only stored for a brief period of time, a preservation regime could assist.

14.133 On the other hand, data retention is general. Data retention regimes require service providers to retain certain types of data for extended periods of time (that is, beyond their usefulness for business purposes) in case that data may one day be required for law enforcement purposes. Three of the types of records that were identified in submissions as being problematic to obtain may only be obtained more readily if a data retention regime was enacted:

- **Cell tower data:** when an electronic device accesses a cell tower, a record of that access is automatically generated indicating the device's location. The New Zealand Telecommunications Forum Inc submitted that this type of record is generated but is not considered to be "readily retrievable" in New Zealand as it would require manual intervention from a qualified engineer to locate and extract it. Therefore we question whether this data would fall under the definition of "document" in the Act, as it is not clear the data is "stored" in the normal course of business. The data could be viewed as being in transit, rather than stored, in which case a data retention regime would be required or an interception warrant would need to be used to obtain it.
- **CCTV footage:** as we explained in Chapter 11, CCTV footage is often obtained from organisations such as local councils and businesses by consent. Submitters commented that sometimes CCTV footage is destroyed before its relevance to an investigation can be identified. Again, only a data retention regime would address this problem.
- **Telecommunications data generally:** it was observed that often crimes are not reported immediately and by the time investigations have commenced, highly valuable telecommunications records may have been destroyed. Again, only a data retention regime could resolve this issue.

14.134 Data retention regimes are highly controversial because they involve wide-ranging collection of personal information, heighten concerns about security and are expensive for service providers to comply with. As we explained in our Issues Paper, Australia and the United Kingdom have data retention regimes. The United Kingdom's original regime in particular was the subject of widespread criticism.

14.135 The regime in the United Kingdom was contained in the Data Retention and Investigatory Powers Act 2014 (UK) (DRIPA). This Act required communications service providers to retain certain call associated data (not content data) and mobile phone location data for up to 12 months. Two Members of Parliament challenged whether the Act complied with European law by taking a case to the European Court of Justice. In December 2016 the Court concluded that the data retention regime in DRIPA "exceeds the limit of what is strictly necessary and cannot be considered to be justified, within a democratic society".¹²³ The Court referred the matter back to the English Court of Appeal for further consideration. In the meantime, the data retention regime in DRIPA has been replaced by a new regime in the Investigatory Powers Act 2016 (UK).¹²⁴ We note that in light of the 2017 terrorist attacks in the United Kingdom, attitudes towards data retention may be shifting.

123 Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson* (CJEU 21 December 2016) at 107.

124 Owen Bowcott "EU's highest court delivers blow to UK snooper's charter" *The Guardian* (online ed, London, 21 December 2016). See also "CJEU judgment in Watson" (21 December 2016) Independent Reviewer of Terrorism Legislation < www.terrorismlegislationreviewer.independent.gov.uk > which states that the judgment in *Secretary of State for the Home Department v Tom Watson*, above n 123, has significance for the Investigatory Powers Act 2016 (UK), as that Act provides for data retention powers similar to (indeed in some respects more extensive than) those contained in the Data Retention and Investigatory Powers Act 2014 (UK).

14.136 In New Zealand, the possibility of enacting a data preservation regime was discussed in the period leading up to the passage of the Telecommunications (Interception Capability and Security) Act 2013. Our understanding is that the preliminary proposals that were discussed were not strictly limited to data that was already stored by service providers in the normal course of business. This raised concerns about data retention, bulk collection of personal information, and cost. As a result, no reform was undertaken at that time.

The Budapest Convention

14.137 In Chapter 12, we recommended that consideration should be given to whether New Zealand should accede to the Council of Europe Convention on Cybercrime (the Budapest Convention).¹²⁵

14.138 The Budapest Convention is the leading international instrument concerning cybercrime. It seeks to address Internet and computer crimes by harmonising national laws, improving investigative techniques and increasing international co-operation. We explained that accession to the Convention would assist New Zealand in determining how best to regulate Internet searches. It would also have wider benefits including enhancing New Zealand's international reputation and creating opportunities to participate in related international negotiations that are currently taking place to improve effective law enforcement and privacy protection in this area.¹²⁶

14.139 As we discussed in our Issues Paper, one of New Zealand's main impediments to becoming a party to the Convention is the fact that it does not have a statutory preservation regime.¹²⁷ The Convention requires member States to have procedures that enable enforcement agencies (by virtue of an order or similar mechanism) to do the following:

- Require a holder of specified stored computer data (including metadata) to preserve and maintain the integrity of that data, in confidence, for a set period of time (up to a maximum of 90 days), pending the execution of a warrant or order. This is particularly desirable where there are grounds to believe that the data is very vulnerable to loss or modification.¹²⁸ It must also be possible to require the holder to disclose the content of any preserved metadata that is necessary to identify the path through which a relevant communication was transmitted, to enable additional relevant data to be identified and preserved.¹²⁹
- At the request of another country that is a party to the Convention, require a holder of specified stored computer data (including metadata) to preserve and maintain the integrity of that data, in confidence, for a set period of not less than 60 days, pending a mutual assistance request.¹³⁰ It must also be possible to require the holder to disclose the content of any preserved metadata that is necessary to identify the path through which a relevant communication was transmitted, to enable additional relevant data to be identified and preserved.¹³¹

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

126 See the discussion in paragraphs [12.88]–[12.103] of Chapter 12.

127 Issues Paper, above n 2, at [9.89].

128 Article 16.

129 Article 17.

130 Article 29.

131 Article 30.

Should the Act be amended to include a preservation regime?

- 14.140 The majority of submitters favoured the inclusion of a preservation regime in the Act. As well as assisting with accession to the Budapest Convention, submitters noted that a preservation regime would create greater certainty for service providers who already preserve data on a voluntary basis. It was also suggested that it would help future-proof the Search and Surveillance Act, as new types of data are constantly being developed and retained in different ways.
- 14.141 Most of those who opposed a formal preservation regime argued that there is simply no need for it. Service providers already preserve data voluntarily. In addition, it would involve twice as much work for enforcement officers (in obtaining a preservation notice and a production order) and for service providers (in preserving the data and then producing it, especially if there is any refinement in terms of scope).
- 14.142 We agree that there is little evidence to suggest that a preservation regime of any kind is necessary for domestic law enforcement purposes. The only area we are aware of where a preservation regime could significantly assist at present is in accessing mobile IP addresses. On its own this might not justify the introduction of a new statutory regime given that the information would only be relevant and available for preservation in a small percentage of the investigations conducted by enforcement agencies each year.
- 14.143 However, we think that a preservation regime would be highly valuable in cases where foreign law enforcement agencies become aware of relevant data that is stored in New Zealand. In such cases, there is a relatively lengthy mutual assistance process that needs to be completed before a New Zealand court can issue a production order. As such, there is a real risk of the data being destroyed in the meantime. Furthermore, accession to the Budapest Convention is not possible unless New Zealand enacts a preservation regime that meets the requirements outlined above.
- 14.144 We therefore recommend that the Act should include a preservation regime that is available to both domestic and foreign law enforcement. As we explain further below, it would be inappropriate for foreign authorities to have access to a greater range of law enforcement tools in New Zealand than domestic agencies.

Our recommended preservation regime

- 14.145 We recommend that the Act be amended to include a tightly constrained preservation regime. This regime should comply with the Budapest Convention, but should not extend significantly beyond those requirements. We want to avoid any suggestion that the regime enables data retention. We are also concerned to ensure that preservation is only ever required in appropriate cases, and is not used as a substitute for applying for a production order in a timely manner. It is important to limit the costs involved in preservation and needless double-handling of data.
- 14.146 In determining the appropriate scope of the regime, we considered and rejected the idea that it should only be available for use in international investigations. As explained above, there does not appear to be a significant domestic case for reform. Instead, our policy objectives are primarily to effectively assist in international investigations and to comply with the Budapest Convention. Nevertheless, we consider that as a matter of principle, foreign countries should not have access to more extensive law enforcement powers in New Zealand than domestic agencies. Further, it appears that a regime with domestic application is required under the Budapest Convention.

- 14.147 To assist in ensuring that the regime is not overused, we recommend that only the Commissioner of Police, a Deputy Commissioner or an Assistant Commissioner should have the power to issue a preservation notice in the first instance. Such a notice should require preservation of specified data, on a confidential basis, for no more than 20 days. This could be extended on application to an issuing officer for up to 90 days, to comply with the Budapest Convention. We think that this is an appropriate compromise between ensuring the data can be preserved straight away and ensuring that any longer periods of preservation (which are likely to be required in international cases) are the subject of external scrutiny. The preservation notice or order should, where appropriate, require the person specified in the order to disclose limited metadata solely for the purposes outlined in the Budapest Convention. Non-compliance with a preservation notice or order should be an offence.
- 14.148 We consider that the Commissioner (or other qualifying senior officer) should be able to issue a preservation notice at the request of any enforcement agency that is entitled to apply for a production order under the Act.¹³² They should also be able to issue an order at the request of the Competent Authority for mutual assistance in New Zealand (the Crown Law Office). The Mutual Assistance in Criminal Matters Act 1992 would need to be amended to enable such a request for preservation to be made and acted upon under that Act. On this point we simply note that the Ministry of Justice is currently reviewing that Act.¹³³
- 14.149 Putting any additional requirements for international requests to one side, we are of the view that a preservation notice or order should only be issued or extended under the Act if the issuer is satisfied that:
- The relevant enforcement agency genuinely intends to apply for a production order in respect of the identified data. This would require the issuer to consider whether the preservation notice or order is as targeted as the subsequent production order would be. The two should align wherever that is possible.
 - The requirements for obtaining a production order are likely to be fulfilled in the circumstances of the case. That is, there must be an offence that is under investigation. A production order also must be available in respect of the type of data that is to be preserved, in the sense that the data must come within the definition of “document” in section 70 of the Act. Finally, it must be likely that the requested documents constitute evidential material and are in the possession or control of the person against whom the preservation notice or order is to be served.
 - Preservation is necessary because the data is particularly vulnerable to loss or modification. This requirement will generally be satisfied where there is insufficient time to obtain a production order before the normal retention period for the identified data expires.
- 14.150 We also considered whether ongoing preservation notices or orders should be available in the same way that forward-looking production orders are available under the Act.¹³⁴ We decided against this approach on the basis that there is no clear evidence of a need for it, and it is not required to comply with the Budapest Convention.

132 We do not think that preservation should be available in respect of any production powers in other legislation. As we have explained in this chapter, those powers are fundamentally different and the Budapest Convention is only concerned with criminal offending, not regulatory offending.

133 This review follows on from the Law Commission’s Report *Modernising New Zealand’s Extradition and Mutual Assistance Laws* (NZLC R137, 2016).

134 Search and Surveillance Act 2012, ss 71(2)(g) and 75(2)(d).

RECOMMENDATION

- R53 Provisions should be inserted into the Act to introduce a new preservation notice regime. That regime should comply with the requirements outlined in the Budapest Convention. The provisions should:
- (a) Enable the Commissioner of Police, a Deputy Commissioner of Police or an Assistant Commissioner of Police to issue a preservation notice.
 - (b) State that a preservation notice requires the recipient to preserve specified data, on a confidential basis, for no more than 20 days. Where appropriate, the notice may also require the recipient to disclose limited metadata to a specified enforcement officer solely for the purposes outlined in the Budapest Convention.
 - (c) Enable an issuing officer to extend the preservation period for up to 90 days.
 - (d) Enable an enforcement officer who can apply for a production order under the Act and the Competent Authority for mutual assistance in New Zealand to:
 - (i) request that a preservation notice be issued; and
 - (ii) apply for the preservation period to be extended.
 - (e) Provide that a preservation notice can only be issued or the period of preservation extended under the Act if the decision-maker is satisfied that:
 - (i) the relevant enforcement agency intends to apply for a production order in respect of the identified data;
 - (ii) the requirements for obtaining a production order are likely to be fulfilled in the circumstances of the case; and
 - (iii) preservation is necessary because the data is particularly vulnerable to loss or modification.
 - (f) Provide that non-compliance with a preservation notice is an offence.

EXTRATERRITORIAL PRODUCTION ORDERS

14.151 In our Issues Paper, we asked whether the Act should be amended to facilitate access to evidence that is stored overseas.¹³⁵ There was some support for that proposal. During consultation, the 2012 case of *Stevenson v R* was brought to our attention as an example of how such evidence could be accessed.¹³⁶ In that case the Court of Appeal rejected a submission that a search warrant issued under section 198 of the Summary Proceedings Act 1957 (the predecessor to section 6 of the Search and Surveillance Act) and forwarded to Microsoft New Zealand (which then forwarded it to Microsoft in the United States) was invalid because it purported to authorise a search in the United States. The Court commented:¹³⁷

The answer to that submission is ... that the Summary Proceedings Act does not require a warrant to be limited to the New Zealand jurisdiction although of course it could not be practically enforced outside of New Zealand.

¹³⁵ Issues Paper, above n 2, question 29. The leading decision on the question of whether a New Zealand statute has extraterritorial effect is *Poynter v Commerce Commission* [2010] NZSC 38, [2010] 3 NZLR 300 at [15] and [78]. See also *Teddy v New Zealand Police* (2014) NZCA 422, (2014) 27 CRNZ 1 at [34]–[59] (leave to appeal to the Supreme Court declined in *Teddy v New Zealand Police* [2015] NZSC 6).

¹³⁶ *Stevenson v R* [2012] NZCA 189, (2012) 25 CRNZ 755.

¹³⁷ At [57].

- 14.152 As discussed in paragraph [14.11] above, prior to the enactment of the Search and Surveillance Act it was common practice to execute a search warrant in respect of a service provider by simply providing them with a copy of the warrant. The production order regime was enacted, in part, to more transparently reflect the nature of the transaction.
- 14.153 Bearing that observation in mind, it was suggested to us that *Stevenson v R* creates a precedent for New Zealand courts to issue extraterritorial production orders. However, we note that if these orders cannot be enforced, this is not a particularly effective law enforcement tool.
- 14.154 Our understanding in relation to the United States is that some service providers do respond to search warrants and production orders that are issued by foreign courts, as long as they relate to metadata such as basic subscriber information or location data. That is because under the Stored Communications Act (US) it is not an offence for a United States-based service provider to disclose this information in certain circumstances.¹³⁸ Accordingly, this might be viewed in the same way that a request for voluntary disclosure of non-sensitive personal information would be treated in New Zealand. The foreign court order simply provides reassurance to the United States-based service provider that disclosure is necessary for law enforcement purposes.
- 14.155 However, if a service provider operates a business in New Zealand but is based in the United States (like in the case of *Stevenson v R*) the service provider may well be in breach of United States law if it complies with a production order that relates to emails or the content of other stored communications. Compliance with the order in those circumstances could breach the Stored Communications Act.¹³⁹ Therefore a production order issued in respect of that information would be ineffective. This is not a theoretical problem. In 2015, a Microsoft executive was arrested in Brazil for failing to hand over data to Brazilian authorities that he was prohibited from disclosing under United States law.¹⁴⁰
- 14.156 As foreshadowed in Chapter 12, the United States is aware of the international frustration that has been caused by the Stored Communications Act.¹⁴¹ To address this issue, it is in the process of passing legislation that would allow its Government to enter into agreements with foreign governments to enable United States-based service providers to comply with foreign search warrants or production orders without breaking United States law.¹⁴² These agreements would be subject to periodic reviews and would expire after five years unless certified otherwise. There are several preconditions.

138 Stored Communications Act 18 USC § 2702(c). In Cybercrime Convention Committee *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for consideration by the T-CY* (September 2016) at [71] and [73] the Cybercrime Convention Committee noted that this “practice of voluntary disclosure” is common and “is specifically foreseen in the Electronic Communications Privacy Act”. (The Stored Communications Act 18 USC is Title II of the Electronic Communications Privacy Act.)

139 Stored Communications Act 18 USC § 2702(a).

140 Jennifer Daskal and Andrew Woods “Congress Should Embrace the DOJ’s Cross-Border Data Fix” (1 August 2016) Lawfare < www.lawfareblog.com > ; David Kris “US Government presents Draft Legislation for Cross-Border Data Requests” (16 July 2016) Lawfare < www.lawfareblog.com > .

141 Chapter 12 at paragraph [12.80].

142 Jennifer Daskal and Andrew Woods “Congress Should Embrace the DOJ’s Cross-Border Data Fix” (1 August 2016) Lawfare < www.lawfareblog.com > .

14.157 First, to enter an agreement the foreign government must have “robust, substantive and procedural protection for privacy and other civil liberties”.¹⁴³ Second, there are certain requirements that must be met in every case, including:¹⁴⁴

- the warrant or order must be issued for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;
- it must be subject to review or oversight by a court, judge, magistrate or other independent authority;
- it must identify a specific person, account, address, electronic device or other specific identifier;
- it must be based on articulable and credible “facts, particularity, legality, and severity regarding the conduct under investigation”;
- it must not relate to the data of a United States citizen, legal permanent resident or person in the United States;¹⁴⁵ and
- there must be a strict prohibition on the dissemination of non-relevant information.

14.158 The United States and the United Kingdom are already in the process of negotiating such an agreement. This would allow the United Kingdom to make a direct request to United States-based service providers for emails and communications information sought in the investigation of crime.¹⁴⁶ The details of this agreement are currently “top secret”.¹⁴⁷

14.159 We consider that this kind of agreement is the appropriate mechanism for dealing with many of the issues surrounding Internet searches that we discussed in Chapter 12. At this stage, it is too early to make any recommendations as to how the Search and Surveillance Act should be amended to facilitate the negotiation of such an agreement with the United States or with other countries that may adopt this model. We do, however, think that accession to the Budapest Convention could assist in demonstrating that New Zealand has sufficiently robust privacy and human rights protections to qualify to negotiate an agreement with the United States. We therefore simply reiterate our recommendation in Chapter 12 that the Government should consider whether New Zealand should accede to the Budapest Convention.

143 Office of Legislative Affairs *Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism* (Washington DC, 2016), s 4(a)(1). The draft provision states that this may be “demonstrated through accession to the Budapest Convention on Cybercrime, or through domestic laws that are consistent with the definitions and the requirements set forth in Chapters I and II of that Convention”.

144 Office of Legislative Affairs *Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism* (Washington DC, 2016), s 4(a)(3).

145 In respect of such data, the usual mutual assistance procedures apply.

146 Jennifer Daskal and Andrew Woods “Congress Should Embrace the DOJ’s Cross-Border Data Fix” (1 August 2016) Lawfare < www.lawfareblog.com > .

147 Alan Travis “Secret report urges treaty forcing US web firms’ co-operation in data sharing” *The Guardian* (online ed, London, 2 June 2015).



Part 4
OTHER
INVESTIGATORY
METHODS

Chapter 15

Covert operations

INTRODUCTION

- 15.1 In this chapter, we discuss how the Search and Surveillance Act 2012 (the Act) should address covert operations. By “covert operations”, we refer broadly to operations in which a person we will call the “agent” interacts with a “target” in order to obtain information by deception (for example, by not disclosing their true motive or identity).¹ The “agent” can be an enforcement officer or another person acting at the direction of an enforcement agency, such as a police informant.² The “target” is a suspect or a person who the enforcement agency believes has information relevant to an investigation. As we discuss below, covert operations cover a wide spectrum of law enforcement activity. The most obvious example is a police undercover or “sting” operation.
- 15.2 Covert operations are a valuable law enforcement tool. They can assist in detecting or obtaining evidence of offending that is otherwise difficult to investigate (for example, because there are no witnesses who are willing to report it or give evidence to support a prosecution). However, some types of covert operations may involve significant intrusions on privacy, similar to searches or surveillance for which a warrant is required.
- 15.3 Covert operations are not currently regulated by the Act, except to the extent that they involve other regulated activity such as interception or visual surveillance. After hearing three cases involving police covert operations in 2015,³ the Supreme Court suggested that there may be merit in introducing a warrant regime or other oversight mechanism for some of the more serious covert operations.⁴
- 15.4 We have reached the view that the Act should include a regime specifically dealing with covert operations. In this chapter we set out proposals to regulate covert operations through a combination of warrants, policy statements and external auditing. These proposals are intended to recognise the legitimacy of covert operations in appropriate cases, while also providing greater transparency and safeguards around their use. They seek to strike a balance between the need for certainty and transparency in the law, and the need for flexibility to allow enforcement agencies to continue to use covert operations in an effective way.
- 15.5 To provide context to these proposals, we first explore the nature of covert operations and give an overview of the current laws that have some bearing on their use.

1 The precise definition of “covert operation” we recommend using in the Act is discussed below at paragraph [15.96].

2 We use the term “agent” here for the sake of simplicity, but note these people are sometimes referred to as “Covert Human Intelligence Sources” (CHIS).

3 *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204; *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705; *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753. We discuss these cases below at paragraphs [15.40]–[15.51].

4 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [127].

THE NATURE OF COVERT OPERATIONS

The element of deception

- 15.6 Covert operations involve the use of deception in order to obtain information from a target that they would not otherwise choose to disclose. This deception can occur in a number of ways. Where the agent is an enforcement officer, the target will generally be unaware of their true identity. The agent may pose as a person who is involved in offending (such as a gang associate or a person interested in purchasing drugs) to gain the target's trust. Where the agent is not an enforcement officer, they may have an existing relationship of trust with the target that the enforcement agency has asked them to exploit. In both cases, the target is deceived about the capacity in which the agent is interacting with them and the purpose of that interaction.

Agencies that conduct covert operations

- 15.7 Covert operations are not only used by New Zealand Police. The Department of Internal Affairs (DIA) conducts online covert operations targeting the distribution of child exploitation material. New Zealand Customs Service officers may also be involved in these operations.⁵ The Ministry for Primary Industries (MPI) uses covert operations to assist in the enforcement of a range of different Acts, particularly the Fisheries Act 1996.
- 15.8 Other enforcement officers may also carry out activity in their day-to-day work that would fall within the definition of covert operations we adopt. For example, an Inland Revenue officer may enter business premises in the same way as a customer in order to observe public-facing activity to better monitor the business' compliance with tax laws.

Purposes for which covert operations are carried out

- 15.9 Covert operations can be used at various stages during investigations to achieve different outcomes. First, they may be used at an early stage, before any specific offences or targets have been identified. The aim in these cases may be to gather intelligence, detect offending or monitor compliance with regulatory regimes. For example:
- Police carries out “controlled purchase” operations, in which people under 18 years of age are asked to attempt to purchase alcohol from various liquor outlets in order to identify outlets that are breaching liquor laws.⁶
 - Police and DIA officers set up covert online profiles in order to identify people engaging in the distribution of child exploitation material or to gather general intelligence about the online forums offenders use to trade in objectionable material.⁷
 - Fisheries officers go undercover as sellers or purchasers of black market shellfish in order to identify people involved in poaching rings.⁸

5 Customs prosecutes offences relating to the importation and exportation of objectionable publications (Customs and Excise Act 1996, s 209). New Zealand Police, Customs and the Department of Internal Affairs work closely together on child exploitation investigations and in some cases may all lay charges against the same person (see, for example, *Webb v R* [2016] NZHC 2966).

6 Liam Cavanagh “More underage stings as cops focus on liquor law breaches in South Canterbury” *The Timaru Herald* (online ed, 19 October 2016); “Alcohol sold to teens in police sting – even after showing correct ID” *The New Zealand Herald* (online ed, Auckland, 15 October 2016); “Underage liquor sting nabs two Nelson stores” *Newshub* (online ed, Auckland, 27 March 2017). An underage person who purchases alcohol does not commit an offence if acting at the request of Police: Sale and Supply of Alcohol Act 2012, s 243.

7 See *Walsh v R* [2016] NZHC 2747; *R v Ottewill* DC Dargaville CRI-2012-011-000261, 1 November 2012. Under ss 124A(2) and 131B(1A) of the Crimes Act 1961, the offences of exposing a young person to indecent material and meeting a young person following sexual grooming apply even if the “young person” is fictitious (that is, a police officer pretending to be a young person).

8 Operation Paid is one example that involved infiltrating an organised pāua poaching ring over 12 months and resulted in charges against 53 defendants: *R v Liu* [2009] NZCA 409; Ministry of Fisheries “Fisheries Officers smash major pāua poaching ring” (27 May 2008) < www.scoop.co.nz >; New Zealand Federation of Commercial Fishermen “Putting Paid to Pāua Poaching” (6 April 2011) < www.nzfishfed.co.nz >. See also Ministry for Primary Industries “Eight people sentenced from MPI's black market bust” (3 May 2016) < www.mpi.govt.nz >.

- 15.10 Second, covert operations can be used for the purpose of investigating specific targets or suspected ongoing offending. Undercover police officers may go to a suspected “tinnie house” asking to purchase cannabis⁹ or infiltrate organised criminal groups; and undercover DIA officers may engage with individuals in online forums where dealing in child abuse material is known to take place to obtain evidence of offending.¹⁰
- 15.11 Finally, covert operations can be used after offending has occurred to obtain evidence to support a prosecution. For example, undercover police officers have been placed in cells with suspects in an attempt to obtain evidence in the form of statements.¹¹ In other cases, undercover officers may use elaborate scenarios to gain a suspect’s trust and seek to obtain a confession. The “Mr Big” technique, which originated in Canada but has been used by Police in New Zealand,¹² is an example of this. It involves undercover officers setting up a bogus criminal organisation, recruiting the target and gaining their trust by involving them in a series of apparently criminal acts in exchange for payment. This may occur over a period of some months. The operation then culminates in an interview with “Mr Big”—the boss of the organisation—for the ostensible purpose of the target gaining full admission to the group. During the meeting, Mr Big tells the target that, in order to join the group, they must be completely honest about their past and promises that any problems associated with prior offending (such as prosecution) will be made to disappear.
- 15.12 Our understanding is that enforcement agencies other than Police do not generally use covert operations for the primary purpose of obtaining evidence of specific offending that has already occurred to support a prosecution (for example, confession evidence). Rather, other agencies’ investigations tend to focus on detecting or investigating ongoing unlawful activity.

A wide spectrum of activities

- 15.13 As is apparent from the examples above, covert operations vary significantly in terms of scale and intrusiveness. At one end of the spectrum, they can form part of the day-to-day activities of an enforcement agency. A food safety officer might pose as a potential customer in order to speak to a person selling meat of dubious origins at a public market. This action might be taken to assist MPI in determining whether any further investigation is required. A covert operation of this kind is short in duration and relatively unintrusive, as the agent does not form a close relationship with the target and is unlikely to obtain highly personal information about them.
- 15.14 At the other end of the spectrum, covert operations can involve numerous agents and targets, elaborate scenarios and may continue over a significant period of time. For example, undercover police officers may infiltrate a criminal gang in order to investigate serious drug and arms offending.¹³ This may require the officer to form close personal relationships with gang members and their associates, enter people’s homes, and in some cases engage in apparent criminal offending in order to maintain a convincing cover story.¹⁴ These larger-scale operations can have a significant impact on the privacy not only of suspects, but also of third parties they associate with who may not be suspected of any wrongdoing.

9 Misuse of Drugs Act 1975, s 34A; *Tararo v R* [2010] NZSC 157, [2012] 1 NZLR 145; *R v Travis* [2012] NZHC 3496; *R v Roberts* HC Whangarei CRI-2008-088-4129, 16 July 2009; Deena Coster “Guilty pleas to drug dealing operation exposed by undercover cops” *Taranaki Daily News* (online ed, 26 May 2016); “Tinnie house exposed by undercover officer” *Marlborough Express* (online ed, 11 November 2014).

10 See Department of Internal Affairs “International operation tracks offender” (14 October 2015) < www.dia.govt.nz > .

11 *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204; *R v Cummings* [2014] NZHC 1025.

12 *L v R* [2017] NZCA 245; *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753; *R v Cameron* [2009] NZCA 87.

13 See, for example, *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705; John Weekes, Jared Nicoll and Virginia Fallon “Grenade, cash, drugs found after undercover officers help in massive Wellington police drug and assets bust” *Stuff* (online ed, Wellington, 11 April 2017).

14 As we discuss below there is a range of offences enforcement officers might commit during undercover operations. Examples include possession of drugs, participation in an organised criminal group and receiving stolen property.

Overview

15.15 There is no legislation in New Zealand that deals with covert operations in any comprehensive way. While covert operations are clearly anticipated by a number of legislative instruments, there is no specific regime that provides for their use or controls the circumstances and manner in which they can be carried out. Instead, there is a patchwork of provisions and legal principles that may affect (directly or indirectly) how covert operations are conducted or how evidence obtained as a result of them is used. Broadly, these fall into the following five categories:

- general principles or obligations that apply to enforcement officers, including the need to act in accordance with the rule of law and the New Zealand Bill of Rights Act 1990 (NZBORA);¹⁵
- provisions in the Search and Surveillance Act that are not specific to covert operations but may affect how such operations are conducted,¹⁶ or that help to protect the safety of undercover officers and informants;¹⁷
- immunity provisions in various Acts that prevent enforcement officers from being prosecuted for certain offences;¹⁸
- rules of evidence that may impact on the admissibility of evidence obtained through covert operations¹⁹ or the manner in which evidence is given by undercover police officers and informants;²⁰ and
- provisions allowing some enforcement officers and informants to obtain specific identity documentation under assumed names (“assumed identity information”).²¹

General principles and obligations applying to enforcement officers

Rule of law

15.16 The rule of law is one of the fundamental principles underlying New Zealand’s constitutional arrangements. While there are many varying definitions of the rule of law, some of its core aspects are generally agreed. The Legislation Design and Advisory Committee summarises them in the following terms:²²

- the law must be clear, accessible and apply to everybody (private citizens and the Government);
- human rights must be adequately protected, and proceedings before courts and tribunals must be fair;
- public powers must be exercised fairly and in accordance with the law, and must never be exercised arbitrarily ...

15 New Zealand Bill of Rights Act 1990, s 3.

16 Search and Surveillance Act 2012, ss 46–47.

17 Search and Surveillance Act 2012, ss 61(3)(b), 62(3)(b) and 98(2)(b).

18 For example, s 34A of the Misuse of Drugs Act 1975.

19 Evidence Act 2006, ss 28–30.

20 Evidence Act 2006, ss 64, 108–109 and 120; Criminal Procedure Act 2011, ss 84, 91 and 94; Criminal Disclosure Act 2008, s 16.

21 Land Transport Act 1998, s 24A; Births, Deaths, Marriages, and Relationships Registration Act 1995, s 65; Electronic Identity Verification Act 2012, s 12.

22 *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) at 12–13. See also Human Rights Commission *Human Rights in New Zealand* (2010) at 89.

- 15.17 The rule of law is not defined in statute. However, its importance is affirmed through references in a number of Acts. The Senior Courts Act 2016 refers to “New Zealand’s continuing commitment to the rule of law”²³ and the Policing Act 2008 states that “principled, effective, and efficient policing services are a cornerstone of a free and democratic society under the rule of law”.²⁴ In addition, the draft Administration of Justice (Reform of Contempt of Court) Bill included in the Law Commission’s recent Report, *Reforming the Law of Contempt of Court: A Modern Statute*, includes “upholding the rule of law” as a principal purpose and objective of the Bill.²⁵
- 15.18 Effective enforcement is necessary to uphold the rule of law. Laws enacted by Parliament constrain, in the interests of the wider public, the manner in which individuals can behave. These laws would lose their potency if enforcement agencies were unable to effectively detect and prosecute non-compliance. Equally, however, the rule of law constrains the manner in which enforcement agencies perform their functions. It means that enforcement officers are bound by the same laws as members of the public except to the extent that the law recognises specific exceptions. For example, they cannot trespass onto private premises or goods without lawful authority;²⁶ and unless a specific immunity applies, they can be liable for criminal offences.
- 15.19 This principle is particularly important in the context of covert operations, in light of the absence of a general statutory regime permitting their use. Under the Search and Surveillance Act, there is a general immunity from civil and criminal liability for any person who acts in good faith and in a reasonable manner to execute a warrant or order, or to exercise a warrantless power.²⁷ That general immunity will not apply to agents conducting covert operations, except to the extent that specific search or surveillance activity forming part of the operation is authorised by warrant or statute. Agents must therefore comply with the civil and criminal laws of the land unless one of the more limited immunities contained in other Acts applies (as we discuss below²⁸).

New Zealand Bill of Rights Act 1990

- 15.20 NZBORA applies to acts done by the executive and any person or body performing a public function, power or duty conferred or imposed by law.²⁹ The rights affirmed in NZBORA may only be subject to “such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society”.³⁰ Where provisions in other enactments can be given a meaning consistent with the rights and freedoms in NZBORA, that meaning must be preferred.³¹
- 15.21 There are two main types of rights affirmed in NZBORA that may be engaged where covert operations are undertaken. First, NZBORA recognises certain rights that are engaged when a person is arrested or detained (due process rights), including the right to refrain from making a statement and to be informed of that right.³² The Supreme Court has held that this right will

23 Senior Courts Act 2016, s 3(2).

24 Policing Act 2008, s 8(a).

25 Law Commission *Reforming the Law of Contempt of Court: A Modern Statute* (NZLC R140, 2017) at 147.

26 *Entick v Carrington* (1765) 19 St Tr 1030, 2 Wils KB 275.

27 Sections 165–167.

28 See paragraphs [15.32]–[15.34].

29 New Zealand Bill of Rights Act 1990, s 3. While covert operatives may not be specifically exercising powers conferred by law, they will be performing functions conferred on the relevant agency (for example, a police covert operation may be for the purpose of law enforcement or maintaining public safety, which are functions of Police pursuant to s 9 of the Policing Act 2008).

30 Section 5.

31 Section 6.

32 Section 23(4).

- be breached where a confessional statement is “actively elicited” by undercover officers from a person who is arrested or detained.³³ In practice, this means that enforcement agencies must exercise caution if they wish to use agents to obtain evidence from a suspect after their arrest (for example, by posing as their cell mates). The courts have not yet determined whether covert questioning of an arrested or detained suspect may breach their right to consult and instruct a lawyer and to be informed of that right,³⁴ although the Chief Justice expressed the view in *R v Kumar* that it does.³⁵
- 15.22 Second, under section 21 of NZBORA every person has the right to be secure against unreasonable search and seizure. Covert operations have not generally been analysed in section 21 terms in case law³⁶ and may not fall obviously within the ordinary meaning of the term “search”.³⁷ However, recent case law has taken the approach that State investigatory activity will be a search for section 21 purposes if it intrudes on reasonable expectations of privacy.³⁸ The Supreme Court has described undercover activity as being potentially “intrusive”.³⁹
- 15.23 The Court of Appeal specifically considered an argument that the actions of an undercover police officer breached section 21 of NZBORA in *Tararo v R*.⁴⁰ In that case the agent went to the front door of a suspected tinnie house and purchased cannabis, wearing a concealed camera to capture the exchange. The Court held that this did not amount to a search. The target’s expectation of privacy was considered to be minimal given that he was willing to sell cannabis to a stranger at his front door.⁴¹ However, the Court recognised that there was “room for a different view on that issue” and said it “would have seen the case in quite a different light if the police officer had entered the house”.⁴²
- 15.24 It seems plausible that the courts may in future find that acts undertaken during the course of a covert operation amount to a “search”. Covert operations have the potential to intrude on any or all of the spatial, personal and informational spheres of privacy.⁴³ Agents may enter people’s homes on the basis of consent that would not be provided if their true identity was known. They may form intimate personal relationships on the basis of deception, which could intrude on personal privacy and dignity. Targets and third parties may also be induced to disclose information to an agent that they could reasonably expect would not be shared, and that they would never willingly disclose to the State. Indeed, the primary purpose of covert operations is to induce the disclosure of information that would not otherwise be disclosed.
- 15.25 If a court did treat acts by an agent as a “search”, the question would then become whether the search was “reasonable”. The degree of intrusion on privacy, the nature of the place or thing

33 *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204 at [27].

34 New Zealand Bill of Rights Act 1990, s 23(1)(b).

35 The majority of the Supreme Court did not express a view on this point: see *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204 at [72]–[73]. Elias CJ considered that there had been a breach of the right to counsel: at [141].

36 With the exception of “participant recording” cases, which we do not discuss in any detail here because participant recording is expressly permitted under s 47 of the Act.

37 For example, Tipping J took the view in *Hamed v R* that the word “search” means “consciously looking for something or somebody” (*Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [220]). However, Blanchard J’s judgment in the same case suggested the ordinary meaning of “search” is broader, capturing the idea of an “investigation or scrutiny in order to expose or uncover” (at [164]).

38 *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [22], discussing the effect of the Supreme Court’s decision in *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305. The Supreme Court declined leave to appeal in *Lorigan*, stating that the Court of Appeal’s decision was a “straightforward and unsurprising application by the Court of Appeal of a decision of this Court”: *Lorigan v R* [2012] NZSC 67 at [2].

39 *R v Wilson* [2015] NZSC 189, [2016] 1 NZLR 705 at [126].

40 *Tararo v R* [2010] NZCA 287, [2012] 1 NZLR 145. The case was appealed to the Supreme Court but on a different issue (*Tararo v R* [2010] NZSC 157, [2012] 1 NZLR 145).

41 At [63].

42 At [63].

43 These “spheres of privacy” were identified by the Supreme Court of Canada in *R v Dymont* (1988) 55 DLR (4th) 503 at 520.

searched and the reasons for the search are relevant to that assessment.⁴⁴ A covert operation could be found to be unreasonable if, for example, the intrusion on privacy involved was considered to be disproportionate to the seriousness of the offending under investigation.

- 15.26 In addition to the rights discussed above, it is possible that other rights affirmed by NZBORA could be engaged by covert operations. In particular, the right to freedom of expression might be relevant in some cases, as it encompasses the right not to impart information.⁴⁵
- 15.27 If an NZBORA right is breached during the course of a covert operation, any evidence obtained as a result will be deemed “improperly obtained” and may be excluded from use in subsequent criminal proceedings under section 30 of the Evidence Act 2006.⁴⁶ This may make the prosecution of offences difficult or impossible. In an extreme case, a proceeding may be stayed to prevent an abuse of process if it is impossible to hold a fair trial or if holding the trial would undermine the legitimacy of the criminal justice system.⁴⁷ A person whose rights have been breached may also be able to claim public law damages in exceptional cases.⁴⁸

Principles provisions applying to enforcement officers

- 15.28 There are general principles set out in legislation that enforcement officers should have regard to in performing their functions, including when carrying out covert operations. For example, the Policing Act 2008 is based on the principles (among others) that policing services are provided in a manner that respects human rights; and that, in providing policing services every police employee is required to act professionally, ethically, and with integrity.⁴⁹ Police employees must also comply with a code of conduct prescribed by the Commissioner of Police.⁵⁰ The principles we have recommended in Chapter 4, if adopted, would also be relevant in the context of covert operations.

Provisions in the Search and Surveillance Act

- 15.29 A number of provisions in the Search and Surveillance Act may apply to some covert operations. A covert operation might include the exercise of warrantless powers or the execution of warrants or orders. For example, if an agent wishes to covertly place a listening device or video camera inside gang headquarters, they would require a surveillance device warrant.⁵¹ Similarly, although there is no express requirement to obtain a warrant to conduct a search, if an agent is asked to carry out an extensive covert search of private premises while the occupier is absent, a search warrant would likely be sought under section 6.
- 15.30 Section 47 contains two exceptions to the requirement to obtain a surveillance device warrant that may apply to enforcement officers carrying out covert operations. First, an enforcement officer who is “lawfully in private premises” does not require a warrant to record what they observe there.⁵² This would allow an enforcement officer who is in private premises with the consent of the occupier during a covert operation to use a listening device or video camera to

44 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [172] per Blanchard J.

45 See Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis, Wellington, 2015) at [13.27.1]–[13.27.4].

46 As occurred in *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204.

47 See the discussion in *R v Wilson* [2015] NZSC 189, [2016] 1 NZLR 705 at [119]–[121].

48 *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA).

49 Policing Act 2008, s 8. These principles do not impose any particular duties on police officers (s 11).

50 Policing Act 2008, s 20; *New Zealand Police Code of Conduct* (May 2015). The Code of Conduct is available at < www.police.govt.nz >. It is high-level and does not contain any guidance specific to covert operations.

51 Search and Surveillance Act 2012, s 46.

52 Section 47(1)(a).

record what occurs.⁵³ Second, a 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”.⁵⁴ This would allow an enforcement agency to intercept phone calls made to or from an agent’s phone. It would also permit an enforcement agency to record conversations between an agent who is not an enforcement officer (such as an informant) and others.

- 15.31 Lastly, a number of the provisions in the Act are designed to maintain the anonymity of agents to protect their safety. Sections 61 and 62 allow a judge, on receiving a report on the use of a surveillance device, to order that the subject of the surveillance be notified in certain circumstances. Such an order must not be made unless the judge is satisfied that the public interest in notification outweighs any potential prejudice to the safety of informants or undercover officers.⁵⁵ Similarly, section 98(2) allows an issuing officer to require an applicant for a search warrant to provide further information about the grounds on which the warrant is sought. However, they must not require disclosure of identifying details of informants unless it is necessary to assess their credibility or whether there is a proper basis for issuing the warrant.⁵⁶

Immunities

Provisions protecting agents from civil and criminal liability

- 15.32 Various Acts contain immunities in relation to specific offences for certain types of enforcement officers. In some cases, these may be relied on in the course of covert operations.
- 15.33 For some enforcement officers—particularly those operating in regulatory contexts—these immunities are already quite comprehensive. For example, the Wildlife Act 1953 contains the following immunity provision:

60 Protection of rangers and others

A person who does any act in pursuance or intended pursuance of any of the functions or powers conferred on him by or under this Act shall not be under any civil or criminal liability in respect thereof, whether on the ground of want of jurisdiction, or mistake of law or fact, or on any other ground, unless he has acted, or omitted to act, in bad faith or without reasonable cause.

Similarly broad immunity provisions can be found in many of the Acts administered by MPI.⁵⁷ Some of these immunities are expressly applied to persons assisting or acting at the direction of enforcement officers.⁵⁸

- 15.34 By contrast, the immunities available to undercover police officers, DIA officers, Customs officers and persons assisting them are much more limited. The broadest immunity we are aware of is in the Misuse of Drugs Act 1975 and prevents the prosecution of undercover police officers for offences against that Act except with the leave of the Attorney-General.⁵⁹ Other immunities or defences are not specific to undercover officers, but apply only to particular offences. For example:

53 The exception only extends to matters the enforcement officer could see or hear without the use of the surveillance device, so it would not permit the officer to leave a surveillance device on the premises after they leave.

54 Section 47(1)(b). In Chapter 9 we recommend this exception be extended to non-oral communications as well (see paragraphs [9.34]–[9.36]).

55 Sections 61(3)(b) and 62(3)(b).

56 “Informant” is defined in s 3 by reference to the definition in s 6(1) of the Criminal Disclosure Act 2008, which states “a person who provides verbal or written information (whether or not in recorded form) to a law enforcement officer”.

57 See the Animal Products Act 1999, s 98; Animal Welfare Act 1999, s 158; Fisheries Act 1996, s 220; Trade in Endangered Species Act 1989, s 52; Food Act 2014, s 351; Forests Act 1949, s 13; Biosecurity Act 1993, s 163; and National Animal Identification and Tracing Act 2012, s 56.

58 See, for example, s 220(2)–(3) of the Fisheries Act 1996.

59 Misuse of Drugs Act 1975, s 34A.

- section 216N of the Crimes Act 1961, which protects constables and Customs officers from liability for making, possessing or publishing an intimate visual recording;
- section 244 of the Crimes Act, which provides a defence to money-laundering charges where the relevant acts were done for the purpose of enforcing specified financial crime legislation;⁶⁰
- section 3(2) of the Arms Act 1983, which provides that nothing in that Act makes it unlawful for police officers to carry or possess firearms, airguns, pistols, restricted weapons, ammunition or explosives;
- sections 243 and 244 of the Sale and Supply of Alcohol Act 2012, which provide that the offence of purchasing alcohol or being present in restricted areas on licensed premises while under the age of 18 does not apply to a person acting at the request of a constable; and
- sections 131(4) and 124 of the Films, Videos, and Publications Classification Act 1993, which provide that the offences of possessing, importing, exporting, distributing and copying objectionable publications do not apply to acts by constables, Customs officers, Inspectors of Publications (who are enforcement officers employed by DIA) or “any other person in the service of the Crown” in the course of their official duties.

Prosecutorial discretion

15.35 Where an agent commits an offence in the course of an investigation and there is no relevant immunity, they will not necessarily be prosecuted. Prosecutors have discretion whether to charge a person with criminal offending.⁶¹ That discretion is exercised in accordance with the Solicitor-General’s prosecution guidelines.⁶² Under the guidelines, a prosecution will only be initiated if it is “required in the public interest” (in addition to there being sufficient evidence to provide a reasonable prospect of conviction).⁶³ Where an offence is committed by an agent in good faith and in a reasonable manner during the course of a covert operation, it is possible that a prosecutor may decide that prosecution is not required in the public interest.

Rules of evidence

15.36 Evidence that is obtained during the course of a covert operation may be excluded from criminal proceedings if it is found to have been improperly obtained.⁶⁴ In addition, statements by defendants will be excluded if they are unreliable⁶⁵ or were influenced by oppression.⁶⁶

15.37 There are also provisions that protect the identity of agents during criminal proceedings. Information about undercover police officers can be withheld during criminal disclosure.⁶⁷ “Informers” (which can include undercover police officers) have a privilege in respect of

60 The legislation referred to is s 243 of the Crimes Act 1961; the Criminal Proceeds (Recovery) Act 2009; the Anti-Money Laundering and Countering Financing of Terrorism Act 2009; and the Financial Transactions Reporting Act 1996.

61 The prosecutor may be an enforcement agency (such as Police) or the Crown. Certain offences must be prosecuted by the Crown (Crown Prosecution Regulations 2013, s 4). The Solicitor-General may also direct any proceeding to be a Crown prosecution.

62 Crown Law Office *Solicitor-General’s Prosecution Guidelines* (1 July 2013) < www.crownlaw.govt.nz > .

63 At [5.1].

64 Evidence Act 2006, s 30. Evidence is “improperly obtained” if it is obtained: (a) in consequence of a breach of any enactment or rule of law by a person to whom s 3 of the New Zealand Bill of Rights Act 1990 applies; (b) in consequence of a statement made by a defendant that is or would be inadmissible if it were offered in evidence by the prosecution; or (c) unfairly (s 30(5)).

65 Evidence Act 2006, s 28.

66 Evidence Act 2006, s 29.

67 Criminal Disclosure Act 2008, s 16.

information likely to disclose their identity.⁶⁸ There are also processes for allowing an undercover police officer to give evidence under their assumed identity.⁶⁹

Assumed identity information

- 15.38 Provision for enforcement agencies to obtain assumed identity information to create or maintain cover identities for agents is currently limited. Driver licences can be issued under assumed names to police employees, witnesses and protected people, and to fisheries officers. There is also an ability to create government-verified electronic identities⁷⁰ and information about births, deaths, marriages, civil unions or name changes⁷¹ under assumed names for undercover police officers, witnesses and protected people.
- 15.39 There is no equivalent provision allowing the issue of passports under assumed names. Nor is there any legislative provision for enforcement agencies to establish corporate entities such as companies to support covert operations. In the absence of express provisions, enforcement officers may be liable for various offences—such as forgery⁷² and making false statements under the Companies Act 1993⁷³—if they create or use documents containing false or misleading information. They may also risk civil liability. Anyone who assists in creating false documents, such as staff in government agencies responsible for issuing identity documents, would also risk liability. If a corporate entity is established, various statutory duties are imposed (for example, on directors under the Companies Act), and failing to comply with those requirements may result in liability.⁷⁴

RECENT SUPREME COURT DECISIONS

- 15.40 In 2015, the Supreme Court considered three cases involving police undercover operations. This series of cases prompted our examination of this issue. They serve to highlight some of the issues that may arise when covert operations are used.

R v Kumar

- 15.41 The first case was *R v Kumar*.⁷⁵ Mr Kumar was a murder suspect who was taken to a police station for questioning. Towards the end of his interview, detectives read out parts of a transcript of a recorded conversation between Mr Kumar and another man. Mr Kumar said he wanted to listen to the full recording with a lawyer present. The interview was terminated and Mr Kumar was arrested. Mr Kumar then instructed a lawyer. The lawyer spoke to a detective, who indicated that Police did not intend to question Mr Kumar again unless new material arose. On that basis, the lawyer said he would speak to Mr Kumar the following morning. Two undercover police officers were then deployed to pose as Mr Kumar's cell mates. They proceeded to ask Mr Kumar questions about the nature of the offending he had been arrested

68 Evidence Act 2006, s 64. An informer is defined as a person who: (a) 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; and (b) is not called as a witness by the prosecution to give evidence relating to that information. They may be a member of Police working undercover (s 64(3)).

69 Evidence Act 2008, ss 108–109 and 120; Criminal Procedure Act 2011, s 84. The process set out in ss 108–109 of the Evidence Act currently only applies in relation to offences punishable by seven years' imprisonment or more, and certain other specified offences. Police and the Ministry for Primary Industries told us this is a problem, as an undercover officer may become a witness to a wide range of offences during a covert operation and the seriousness of the offence may not reflect the level of danger to the officer. The Law Commission will consider that issue as part of its current review of the Evidence Act 2006, which is due to be completed by February 2019.

70 Electronic Identity Verification Act 2012, s 12 (this relates to the government's RealMe identity verification service).

71 Births, Deaths, Marriages, and Relationships Registration Act 1995, s 65.

72 Crimes Act 1961, ss 265–259.

73 Companies Act 1993, s 377.

74 Companies Act 1993, s 374.

75 *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204.

for, eventually asking him why he had burned the body. The Crown sought to rely on Mr Kumar's statements in his subsequent trial.

- 15.42 The Court unanimously found that the statements by the defendant had been obtained in breach of the right to refrain from making a statement in section 23(4) of NZBORA and should be excluded under section 30 of the Evidence Act. In determining that section 23(4) had been breached, the majority of the Court adopted the test of whether the undercover officer “actively elicited” information or “prompted, coaxed or cajoled” the suspect such that the questioning amounted to the “functional equivalent of an interrogation”.⁷⁶
- 15.43 In applying this approach to the circumstances of the case, the Court stated:⁷⁷

An undercover officer is entitled to engage a detainee in conversation. But he or she may not conduct the functional equivalent of an interrogation. Whether the officer has done so is to be assessed in terms of what the officer actually did – the sequence and nature of the questions asked, their relevance to the police investigation, how persistent the officer was and so on. The court should not speculate on what might have happened if the officer had been a genuine inmate or had taken a low-key role. The danger of such an approach is that it could allow what is the functional equivalent of an interrogation on the basis of the court's assessment that the detainee is a naturally talkative and outgoing person who would have engaged with fellow detainees in any event. Adopting such an analysis would undermine the protected rights at issue.

Wilson v R

- 15.44 The second case was *Wilson v R*.⁷⁸ This case involved the use of an undercover police officer as part of Operation Explorer, which investigated the activities of the Red Devils motorcycle gang. At issue was the use of a bogus warrant and prosecution (collectively referred to by the Court as the ‘scenario’) to strengthen the undercover officer's credibility with the gang. The scenario first involved creating and executing a false search warrant in relation to a storage unit rented in the name of the undercover officer, in which Police had placed apparently stolen items and equipment consistent with cannabis offending. A staged arrest and false prosecution of the officer followed, including several court appearances. The then Chief District Court Judge was approached to request approval for the undercover officer to appear in court under an assumed name.⁷⁹
- 15.45 The procedural history of the case was described by the Supreme Court as “unusual”.⁸⁰ Shortly put, the issues before the Supreme Court were whether the Court of Appeal had erred in

76 *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204 at [43]. Elias CJ agreed with the result but took a different approach to when s 23(4) would be breached. She considered the undercover officers could only have avoided breaching s 23(4) if they had been purely “passive observers” (at [125]).

77 *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204 at [62].

78 *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705.

79 The precise nature of the approval by the Chief District Court Judge was disputed on appeal. However, the High Court finding that the judges who dealt with the undercover officer during his court appearances believed the prosecution was real was not contested.

80 *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705 at [29]. Mr Wilson had originally been charged with 20 others. Their application to the High Court for a stay of prosecution (based on the use of the bogus scenario) was part heard when Mr Wilson asked for a sentence indication and then entered a guilty plea for his charges. The subsequent High Court decision (*R v Antonievic* [2012] NZHC 2686) granted a stay in respect of his co-defendants. Mr Wilson then sought to appeal his conviction and sentence, seeking leave to vacate his guilty plea in the light of the High Court decision. Meanwhile the High Court decision to stay proceedings was appealed to the Court of Appeal and overturned in *R v Antonievic* [2013] NZCA 483, [2013] 3 NZLR 806 and the charges against the co-defendants remitted for trial. Mr Wilson then proceeded only with the appeal against sentence: *Wilson v R* [2014] NZCA 584. In the trial of the remaining co-defendants, rulings (not appealed by the Crown) were made under s 30 of the Evidence Act that the evidence obtained as a result of the scenario should be excluded in relation to both non-serious and serious charges. Fresh stays of proceedings were issued in relation to the serious charges, based on the High Court's view that important pieces of evidence had not been available to the Court of Appeal: *R v Antonievic* [2015] NZHC 1096. The High Court later discharged the defendants on the non-serious charges under s 347 of the Crimes Act 1961. The net result was that proceedings against all co-offenders were either stayed or discharged for lack of evidence. Mr Wilson then filed an application for leave to the Supreme Court.

overturning the stay of proceedings⁸¹ against the other defendants that had been granted by the High Court and, if so, whether the appellant should be granted leave to withdraw his guilty plea on that basis. The stay of proceedings had been granted on the basis that Police impropriety in creating the false warrant, bringing false charges and involving the Chief District Court Judge amounted to an abuse of process.

- 15.46 The majority of the Supreme Court agreed the scenario constituted serious misconduct, stating:⁸²

We well understand that the police face difficulties in investigating certain types of offending, including organised drug offending. But that cannot justify preparing and using bogus search warrants or bringing bogus prosecutions in the courts. If the public are to have confidence in the rule of law, they must have confidence in the independence of the judiciary and the genuineness of court processes. The bogus warrant/bogus prosecution scenario had the capacity to undermine that confidence significantly.

- 15.47 However, after undertaking a balancing exercise the majority ultimately agreed with the Court of Appeal that the original stay of proceedings should not have been granted.⁸³ While that effectively disposed of the ground of appeal, the majority acknowledged that a question of fairness arose from the fact that prosecutions had been freshly stayed against virtually all other defendants (as a result of litigation that the Crown had not appealed). The Court therefore quashed the convictions on the basis that to allow them to stand would constitute a miscarriage of justice.

R v Wichman

- 15.48 The final case was *R v Wichman*.⁸⁴ That case involved a “Mr Big” undercover operation, which culminated in the target admitting to shaking his infant daughter causing her death.⁸⁵ The issue on appeal was whether evidence of the admission should have been excluded on the basis that it was unreliable⁸⁶ or improperly obtained.⁸⁷ The Court was split 3:2, with the majority concluding that the evidence was admissible. The majority recognised that Mr Big operations had the potential to result in false confessions,⁸⁸ but concluded that it had been open to the trial Judge to find that the statement at issue in that case was reliable.⁸⁹
- 15.49 In giving the judgment of the majority, William Young J suggested an authorisation or oversight regime may be appropriate for undercover operations. Given the importance of these observations to the issues we are considering, we set them out in full:

[126] As will already be apparent, we have had to address three cases this year which have involved significant issues about other undercover operations. Experience has shown that there is potential for undercover operations to go awry, particularly where an undercover officer becomes part of the life of a suspect or the associate of a suspect in respects which are very intrusive. Such operations may

81 A stay of criminal proceedings may be granted where there is a state of misconduct that will (a) prejudice the fairness of the defendant’s trial or (b) undermine public confidence in the integrity of the judicial process if a trial is permitted to proceed: see *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705 at [40].

82 *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705 at [91].

83 At [93].

84 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753.

85 The “Mr Big” technique is described above in paragraph [15.11].

86 Evidence Act 2006, s 28.

87 Evidence Act 2006, s 30.

88 At [74].

89 At [92]. The Court of Appeal had reached a contrary conclusion, noting that there was no independent evidence to confirm the likely truthfulness of the confession (*M v R* [2014] NZCA 339, [2015] 2 NZLR 137). (Under s 28 of the Evidence Act 2006, where a defendant raises the issue of reliability of a statement and provides an evidential foundation for it, the judge must exclude the statement unless satisfied on the balance of probabilities that the circumstances in which the statement was made were not likely to have adversely affected its reliability.)

have detrimental effects on the suspect. There has been much controversy as to this in the United Kingdom particularly where male undercover officers have formed long-term sexual relationships with female members of the group under investigation which in some instances have resulted in children. A similar situation (involving sexual relationships but not children) has arisen in New Zealand. There are also the different issues which arose in *Wilson* as to the nature of the steps taken to avert suspicion of the undercover officers. Human nature being what it is, the police officers who design and run undercover operations are likely to be primarily focused on securing a successful outcome and there is an associated risk, which has sometimes crystallised, that other important and countervailing considerations are not sufficiently taken into account.

[127] The case by case approach which this Court must take in relation to the appropriateness of particular police practices is not well-suited to the establishment of general guidelines as to the circumstances in which a particular investigatory technique is deployed. 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.

- 15.50 These observations were made in the context of a case concerning a Mr Big operation. These types of cases raise specific issues that may not apply to other undercover operations. They may raise questions of unreliability of confessions (based on the circumstances in which the statement is made), unfair prejudice to the defendant (because the evidence from a Mr Big scenario will demonstrate a willingness on their part to engage in offending) and breach or avoid constraints on police interrogation (which would apply if the person were in actual police custody or being questioned by Police). However, we consider the majority's comments about the potential for undercover operations to be highly intrusive are relevant to other kinds of covert operations as well.
- 15.51 Both Elias CJ and Glazebrook J in their separate dissenting judgments also commented on the risks associated with Mr Big operations, although neither expressed a view on whether an authorisation regime should be introduced.⁹⁰

CONSULTATION

Issues Paper

- 15.52 In our Issues Paper we discussed covert operations under the heading of “in-person surveillance”, by which we referred to the observation or monitoring of a person, place or thing by enforcement officers (rather than by electronic means). Not all such activity would fall within our definition of “covert operations”. The definition depends on the establishment or maintenance of a relationship for a covert purpose, which requires engagement with a target. Other types of in-person surveillance—for example, following a person to observe their movements—are discussed in Chapter 11.
- 15.53 We noted that covert operations raise a number of difficult issues.⁹¹ They have the potential to involve breaches of the law by undercover officers. They also carry a risk that confessions will be excluded from subsequent proceedings because the usual safeguards on questioning suspects (such as informing arrested or detained persons of their right to refrain from making a statement) cannot realistically be complied with.

90 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [293] and [307] per Elias CJ and at [403] per Glazebrook J.

91 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.80]–[3.81] [Issues Paper].

- 15.54 We referred to the fact that the United Kingdom and Australia have authorisation regimes that deal with covert operations.⁹² We suggested that some covert operations can be at least as intrusive as (if not more intrusive than) types of surveillance that require a warrant, such as interception.⁹³ It is arguably anomalous that there is no authorisation regime in New Zealand that deals with them. We indicated our preliminary view that an authorisation framework would help to prevent breaches of suspects' due process rights; protect individuals' privacy; ensure appropriate use of State resources; ensure covert operations are carried out in such a manner that the evidence obtained is likely to be admissible; and provide a clearer legal mandate for enforcement agencies.⁹⁴
- 15.55 We sought submitters' views on whether the Act should regulate in-person surveillance (including covert operations) and, if so, how that should be done.

Submissions

- 15.56 Submitters were roughly evenly split on whether covert operations should be regulated. Enforcement agencies were mostly opposed to any requirement to obtain authorisation for covert operations. They emphasised the need for flexibility, since it often cannot be known in advance how a covert operation will develop. They also pointed out that "covert operations", broadly defined, may capture many routine law enforcement activities; may occur at an early stage in an investigation where the threshold for a warrant will not be met; and may not involve enforcement officers doing anything unlawful. Requiring authorisation for all such activities would cause significant delay and prejudice effective law enforcement. On the other hand, Police (and DIA and Customs in subsequent discussions) did request broader immunities for agents.⁹⁵ Police also supported the introduction of an assumed identities regime.
- 15.57 Most non-enforcement agency submitters favoured authorisation for at least some covert operations. They noted these operations can involve a high level of intrusion. Agents may acquire similar data to a listening device, but in a more intimate way. They also observed that where a covert operation involves breaches of the law by agents, this may undermine fundamental rights and the rule of law. However, there was no clear consensus on the appropriate form or scope of any authorisation regime.
- 15.58 Most of the members of our Expert Advisory Group also supported the introduction of a warrant regime for more serious covert operations, provided this could be done in a way that would be reasonably practicable for enforcement agencies.
- 15.59 Following the receipt of submissions on our Issues Paper, while developing our recommendations, we continued to engage with enforcement agencies that frequently conduct covert operations. During these discussions, Police and DIA advised us that they would support an authorisation regime for covert operations if it was sufficiently flexible and warrants were only required where agents might commit offences for which they do not currently have immunities. MPI and Customs did not support an external authorisation regime for the covert operations they conduct. Customs indicated it would be comfortable with an independent auditing process for only those covert operations that might rely on new immunities conferred under the Act. MPI is in a different position to the other agencies because its officers already

92 At [3.84]–[3.97].

93 At [3.98]–[3.99].

94 At [3.100]–[3.102].

95 We discuss this in further detail in paragraphs [15.76]–[15.77].

have extensive immunities for the regulatory offences they may need to commit during covert operations.⁹⁶ It did not seek any additional immunities.

THE CASE FOR REGULATING COVERT OPERATIONS

Risks associated with covert operations

- 15.60 As is apparent from the Supreme Court cases discussed above, there are particular risks associated with covert operations that may give rise to legal challenges. The first and second risks discussed below are largely confined to cases where an agent is seeking to obtain confession evidence in relation to a crime that has already occurred. The third and fourth risks can apply to covert operations more generally.
- 15.61 First, covert operations aimed at securing incriminating statements may give rise to concerns about reliability.⁹⁷ Agents may exert pressure on a target to disclose information. Some of the Canadian Mr Big operations have used scenarios intended to portray to the target that the members of the bogus criminal group will use violence against anyone who betrays their trust.⁹⁸ In New Zealand, scenario operations have been carefully planned to avoid any suggestion of violence, but inducements may be offered to encourage disclosure. For example, the target may be offered financial incentives to join or remain in the criminal group⁹⁹ and promised that if they admit to offending they will not be prosecuted.¹⁰⁰
- 15.62 The Supreme Court observed in *Wichman* that inducements of this kind create a real possibility of a false confession. William Young J, giving the judgment of the majority, said:¹⁰¹
- Inherent in a Mr Big operation is putting the suspect under pressure to confess in a context in which the suspect is led to believe that such a confession will bring about the benefits associated with membership of the organisation without resulting in adverse consequences. It is not inconceivable that an innocent target of a Mr Big operation might be induced to make a false confession. It is possible that, at least in some circumstances, the risk of a confession obtained from this sort of operation being false may be as great – if not greater – than the corresponding risk associated with a confession obtained during a custodial interrogation. The fact that a suspect is not in custody and does not perceive the questioner as having the coercive power of the state at their disposal is not a complete answer to concerns as to reliability. Nor does the fact that the technique relies on psychological rather than physical pressure mean that such pressure could not, in the right circumstances, be seen as coercive. We are very aware of this risk. As we have pointed out, there are examples from Canada that suggest that it has crystallised on occasion.
- 15.63 Second, in addition to reliability concerns, scenario operations in which the defendant is convinced to participate in apparently criminal activity can potentially prejudice a subsequent trial. That is because it shows a willingness on the part of the defendant to engage in offending, which may influence a jury.¹⁰²
- 15.64 Third, covert operations have the potential to breach or undermine rights recognised by NZBORA. Depending on the circumstances, this could include due process rights (such as the

96 See paragraph [15.33].

97 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [20]; *R v Hart* 2014 SCC 52, [2014] 2 SCR 544 at [68]–[69].

98 See, for example, *R v Hathaway* 2007 SKQB 48, 292 Sask R 7.

99 See *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [157] and *L v R* [2017] NZCA 245 at [55] (although the Court of Appeal in *L v R* did not consider the inducements offered in that case were significant: at [60]).

100 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [158] and *L v R* [2017] NZCA 245 at [24].

101 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [74].

102 At [21]; *R v Hart* 2014 SCC 52, [2014] 2 SCR 544 at [73].

right to refrain from making a statement) or the right to be secure against unreasonable search and seizure.¹⁰³

- 15.65 The fourth risk relates to the propriety of conduct carried out by State agents. In seeking to create or maintain an effective cover story or elicit information, there is a risk that agents may carry out activity that breaches the law or amounts to an abuse of process.¹⁰⁴ If this kind of activity by the State is allowed to occur without clear, consistent and transparent rules, it could be seen to undermine the rule of law and the integrity of the criminal justice system.

Level of intrusion on privacy

- 15.66 As we discussed in Chapter 4, one of the basic premises underlying the Act is the presumption that activity that intrudes on reasonable expectations of privacy should be specifically authorised. We have recommended the inclusion of an explicit provision in the Act requiring enforcement officers and issuing officers to have regard to that principle.¹⁰⁵ We have also noted above that covert operations could be found to involve activity that amounts to a “search” in terms of section 21 of NZBORA due to their potential to intrude on reasonable expectations of privacy.¹⁰⁶
- 15.67 As with any category of search or surveillance, covert operations will involve varying levels of privacy intrusion. In some cases the interaction between the agent and the target will be fleeting and the agent will glean no more information than the target would be willing to disclose to any member of the public. This may be the case where an enforcement officer from a regulatory agency speaks to a business owner or employee while posing as a customer. The level of privacy intrusion involved in these cases is likely to be low.
- 15.68 In other cases, the agent will form close and trusting relationships with targets and third parties over a significant period of time. The target may invite the agent into their home, form close relationships with them and share highly personal information. In such situations the intrusion on privacy may well be greater than in the case of interception or visual surveillance. The intrusion may continue for a longer period of time¹⁰⁷ and the target may be induced to disclose information they would not otherwise have volunteered. The element of betrayal of trust involved in these types of covert operations can also be seen as an affront to personal privacy and dignity.
- 15.69 As the Supreme Court has observed, “sanction in the form of a warrant is required for police investigations which are far less intrusive than a Mr Big operation”.¹⁰⁸ In our view, that observation should not be limited to Mr Big cases. Operations that aim to detect offending, such as where agents infiltrate criminal groups, may involve similar levels of intrusion. The intrusion stems from the nature of the relationships formed between the agent and the targets (or their associates), not the ultimate goal of the operation.

Existing laws do not adequately prevent breaches of rights

- 15.70 Exclusion of evidence is the primary remedy where a covert operation is found to have been conducted improperly or a confession is considered to be unreliable.¹⁰⁹ However, as we

103 See paragraphs [15.20]–[15.27].

104 *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705 at [40].

105 Chapter 4 at paragraphs [4.23]–[4.24].

106 See paragraphs [15.22]–[15.27].

107 Surveillance device warrants are valid for a maximum of 60 days (s 55(1)(c)), whereas covert operations are not subject to any time limits.

108 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [127].

109 Evidence Act 2006, ss 8 and 28–30. See paragraphs [15.27] and [15.36].

explained in Chapter 2, exclusion of evidence does not prevent breaches of rights from occurring and is not a sufficient accountability mechanism where improper State conduct occurs.¹¹⁰ This is true generally, but is particularly pronounced in relation to covert operations because they can occur at an early stage in an investigation or for intelligence-gathering purposes. The information obtained may be used to inform internal agency decisions about where to focus resources, or relied on in applications for warrants. It may not be relied on as evidence in proceedings, in which case admissibility issues will never arise.

- 15.71 Where information obtained from a covert operation is not relied on as evidential material, the operation usually will not be disclosed outside of the enforcement agency. Unlike searches carried out under a warrant, there are no requirements to provide notice to persons affected.¹¹¹ Even in the case of surveillance, which is always conducted covertly, a judge can order that a target be notified if the judge has concerns about the propriety of the surveillance.¹¹² Enforcement agencies are also required to report annually on the use of surveillance device warrants, warrantless powers, declaratory orders and examination orders.¹¹³
- 15.72 The secrecy surrounding covert operations makes it less likely that any misconduct will be open to challenge. People whose rights are breached during an operation may never realise what actually occurred, so cannot make complaints or file proceedings seeking redress. Nor will oversight bodies such as the Independent Police Conduct Authority necessarily become aware of any improper conduct, so the opportunity for enforcement agencies to be held accountable is limited.
- 15.73 Furthermore, some of the protections the law imposes to prevent rights breaches are not engaged where covert operations are carried out. For example, ordinarily police officers must inform a person of their right to refrain from making a statement and to consult a lawyer before questioning them if there is sufficient evidence to charge them, or if they are in custody.¹¹⁴ These requirements do not apply to undercover officers, and could not realistically be met without prejudicing the investigation.¹¹⁵ The fact that a target need not be cautioned before being questioned by an agent may increase the risk that the rights in section 23 of NZBORA will be undermined.¹¹⁶ As one commentator has suggested:¹¹⁷

Statutory regulation may not reverse the trend towards undercover policing. It may, however, redirect the focus and enhance the legal accountability of undercover policing: the current state of under-regulation simply encourages its use as a means of evading or neutralizing the due process protections ordinarily available to suspects during custodial investigation.

- 15.74 In our view, the current legal framework provides insufficient checks in an area as potentially intrusive as covert operations. The public should be able to see that appropriate steps are being taken to ensure their rights are protected and any breaches will be addressed.

110 See paragraphs [2.70]–[2.72].

111 Search and Surveillance Act 2012, s 131.

112 Sections 61–62.

113 Sections 170–172.

114 *Practice Note – Police Questioning (s 30(6) of the Evidence Act 2006)* [2007] 3 NZLR 297; New Zealand Bill of Rights Act 1990, ss 23(1)(b) and 23(4).

115 *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [106] and [112]. See also *R v Hart* 2014 SCC 52, [2014] 2 SCR 544 at [79].

116 For example, where a statement is “actively elicited” from a suspect: *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204 at [27]. See also *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753 at [113]–[114].

117 Simon Bronitt “The Law in Undercover Policing: A Comparative Study of Entrapment and Covert Interviewing in Australia, Canada and Europe” (2004) 33 *Comm L World Rev* 35 at 80.

The legal boundaries of covert operations are unclear

- 15.75 As we have explained above, the immunities available to some enforcement agencies are currently limited. Where no immunity applies, prosecutorial discretion determines whether an agent will face criminal charges. This obscures the legal boundaries of covert operations, creating potential uncertainty for enforcement agencies, other actors in the criminal justice system and the public. Similarly, the extent to which enforcement agencies can obtain assumed identity information outside the current limited provisions is unclear.
- 15.76 Police and DIA drew our attention to a number of offences that their officers do not have immunity in respect of, but that they may be at risk of committing in order to carry out covert operations effectively. For example, undercover police officers who infiltrate a gang may commit the offence of participation in an organised criminal group.¹¹⁸ They may also be at risk of committing crimes such as receiving stolen property in order to maintain their cover.¹¹⁹ In addition, agents and people assisting them risk liability for forgery offences if they make or use false documents to maintain a cover story.¹²⁰ Currently there are no immunities applying to these offences.
- 15.77 For DIA, the main issue is that section 124A of the Films, Videos, and Publications Classification Act 1993 only protects enforcement officers who distribute objectionable material if the distribution is to another person who is in the service of the Crown.¹²¹ In order to effectively identify and locate people who are trading in objectionable material, enforcement officers may need to distribute objectionable material to people who do not fall within that category.¹²² This is also an issue for police officers and Customs officers, who work closely with DIA on child exploitation investigations. DIA also requested immunity from the computer misuse offences in the Crimes Act 1961,¹²³ to allow it to disrupt online platforms that are used to trade in objectionable material.
- 15.78 We recognise that, even if more immunities are introduced, situations may arise during a covert operation that are not anticipated. An agent may become implicated in offences that are not covered by the immunity provisions. In those cases it is appropriate that prosecutors continue to assess whether prosecution is required in the public interest, having regard to the facts of the particular case.
- 15.79 However, where it is possible to identify offences that agents are likely to become involved in, in our view, it is preferable for Parliament to consider whether enforcement officers and/or persons acting at their direction should have immunity for those offences. Statutory immunity provisions provide greater transparency for the public and greater certainty for enforcement officers than reliance on prosecutorial discretion.

Internal guidance is insufficient

- 15.80 Given the intrusive and highly resource-intensive nature of some covert operations, it is important for both the public and enforcement agencies that they are only initiated in appropriate cases and are carried out in such a manner that the evidence obtained is likely to be admissible in any subsequent trial.

118 Crimes Act 1961, s 98A.

119 Crimes Act 1961, s 246.

120 Crimes Act 1961, ss 265–259.

121 Films, Videos, and Publications Classification Act 1993, s 124A(1)(c).

122 Films, Videos, and Publications Classification Act 1993, ss 123–124.

123 Crimes Act 1961, ss 250 and 252.

- 15.81 Police and MPI assured us that they have robust internal processes and policies in place to ensure this occurs. We were not able to see the content of these policies—due to concerns that it might prejudice sensitive investigatory methods—so we cannot comment on their adequacy. However, irrespective of their content, we think it is undesirable to rely entirely on each individual agency assessing what is appropriate, without the benefit of Parliamentary guidance, independent external approval or review, or any consistent policy across government.
- 15.82 We have concluded that the lack of regulation of covert operations is undesirable. Increased transparency and accountability is required to ensure that intrusive State powers are exercised in accordance with the rule of law and to encourage public confidence in the integrity of the criminal justice system. Public mandate is critical for enforcement agencies to operate effectively – both to reflect the principles of constitutional democracy and for more practical reasons. Members of the public may be more willing to provide information to an enforcement agency or to act as a Crown witness in a prosecution if they respect the manner in which the agency operates.

OVERVIEW OF OUR PROPOSED COVERT OPERATIONS REGIME

- 15.83 Australian commentator Clive Hartfield has suggested that professionalism in the covert investigations area can be aligned with the following four principles:¹²⁴
- Evidence to sustain a prosecution or intelligence to facilitate investigation management must be obtained in a manner that preserves the integrity of the criminal justice system and its actors.
 - Statutory rights of the suspect should not be breached except when the following criteria are met in full: the rights are qualified, breach is necessary and there is statutory authority to do so.
 - The rights and privacy of those citizens not suspected of criminal conduct must be protected: collateral harm as a consequence of covert investigation should be minimised through effective investigation management.
 - The professional integrity of investigators must be demonstrated, or, if necessary, its absence exposed.
- 15.84 We would add an additional principle: that covert operations should be carried out in a manner that minimises the risk of obtaining unreliable evidence (such as false confessions). These principles flow from the concerns we have discussed above. We think they provide an appropriate starting point for assessing the goals of a statutory regime for covert operations. It would, of course, be possible for an agency to give effect to these principles through its own internal processes. However, because these internal processes are currently not transparent, there is no way for the public to know if that is the case. An effective statutory framework should encourage transparency and consistent compliance with these principles across government.
- 15.85 To achieve that, in our view, the statutory regime needs to include two features:
- Prospective constraints on the circumstances and manner in which covert operations can be used. We recommend that this occur through a combination of warrants issued by an independent judicial actor and policy statements providing guidance to enforcement officers.
 - Accountability mechanisms to ensure that any inappropriate practices are identified and addressed, and that steps are taken to prevent future mistakes. We propose to achieve this through an external auditing process and by requiring agencies' policy statements to be made public.

124 Clive Hartfield "The Governance of Covert Investigation" (2010) 34 *Melb U L Rev* 773 at 783.

- 15.86 We also recommend the introduction of more comprehensive immunity and assumed identity regimes, to clarify the legal boundaries of covert operations.
- 15.87 We do not intend our recommendations to prevent or discourage enforcement agencies from carrying out covert operations. They are an important investigatory tool that may allow agencies to detect or prosecute offending that might otherwise go unchecked. Our proposals recognise that it is in the public interest that enforcement agencies be able to use covert operations, provided that use is subject to defined limits.

COVERT OPERATIONS WARRANTS

- 15.88 As we have discussed,¹²⁵ covert operations cover a wide spectrum of enforcement activity. Activities at the lower end of that spectrum may involve only fleeting interactions with targets and form part of the day-to-day practices of enforcement agencies. Any statutory regime needs to properly account for this. Requiring a warrant to conduct any activity (no matter how fleeting) that involves an agent interacting with a target to covertly obtain information would be unworkable. The cost and delay involved would prevent enforcement agencies from doing their jobs effectively.
- 15.89 We initially favoured the idea of requiring enforcement officers to obtain a warrant before conducting more intrusive covert operations. However, we had difficulty in selecting criteria that could accurately determine which operations are sufficiently “intrusive” to require authorisation. We tested a range of possible criteria with enforcement agencies. It became clear during those discussions that any statutory requirement to obtain a warrant would either be arbitrary (for example, the length of time an operation continues for) or too vague (such as whether the operation will intrude on reasonable expectations of privacy). They would likely capture too many cases, constraining everyday enforcement activity, or too few cases, so that some quite invasive operations would not be captured.
- 15.90 To provide one example, in Australia and the United Kingdom a distinction is drawn between short-term covert operations, which can be approved internally by a senior member of an enforcement agency,¹²⁶ and long-term operations, which must be externally approved.¹²⁷ We are not convinced that the length of time an operation continues for necessarily reflects the level of risk¹²⁸ or privacy intrusion it involves. An operation may continue for years but involve only one or two interactions with a target per year. On the other hand, an operation that continues for only a short period may carry a high risk that rights will be undermined (for example, where an arrested person is questioned by undercover officers) or that agents will be involved in significant offending (for example, if an agent becomes a party to offending by an organised criminal group).
- 15.91 This led us to conclude that the warrant provisions should be empowering rather than mandatory, like the search warrant regime. In practice, this would mean enforcement officers need to obtain a warrant where an operation may involve unlawful activity and the enforcement officer wishes to have the benefit of immunities under the Act.¹²⁹ In other cases, a warrant would be available but not required.

125 See paragraphs [15.7]–[15.14].

126 Crimes Act 1914 (Cth), ss 15GF and 15GI; Regulation of Investigatory Powers Act 2000 (UK), ss 29–30.

127 Crimes Act 1914 (Cth), s 15GU; Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 (UK), cls 3 and 5. Long-term operations are those exceeding three months, in Australia, or 12 months, in the United Kingdom.

128 The types of risks associated with covert operations are discussed in paragraphs [15.60]–[15.65].

129 We discuss immunities at paragraphs [15.140]–[15.145].

- 15.92 We acknowledge this will mean the Act does not specifically require a warrant for some covert operations that may be quite intrusive. An operation could continue for a long time and involve significant invasions of privacy without involving any unlawful activity.¹³⁰ However, our recommendations in this chapter must also be viewed alongside the principles provision we have proposed. In line with those proposals, enforcement officers would be required to take into account the principle that intrusive activity should be carried out pursuant to statutory mechanisms (including policy statements).¹³¹ In the covert operations context, any potential impact on due process rights and the risk of obtaining unreliable confessions should also be considered.
- 15.93 We would encourage agencies to seek a warrant before carrying out a covert operation if there is significant doubt about whether it may breach or inappropriately circumvent rights recognised in NZBORA. Like declaratory orders, obtaining a covert operations warrant in these situations should provide a measure of assurance to the agency that the proposed operation, if carried out as planned, will be reasonable and the evidence obtained as a result will be admissible. The fact that a warrant was obtained and complied with may also be a relevant consideration for a later court determining the admissibility of evidence.¹³² However, we do not intend this to become a default requirement to obtain a warrant. The practicalities of policing need to be borne in mind, and we recognise it will not be realistic to obtain a warrant in every case where a reasonable expectation of privacy is engaged.
- 15.94 As we discuss below,¹³³ policy statements and auditing requirements will assist in ensuring covert operations are used appropriately, and will be particularly important in cases where a warrant is not obtained. We envisage that policy statements would also provide more detailed guidance on when warrants should be sought, in light of the types of covert operations carried out by particular agencies.

Defining “covert operations”

- 15.95 Because we are not recommending that a warrant be *required* to carry out any covert operation, it is appropriate that covert operations be defined in a broad way. This will ensure that warrants can be sought by enforcement officers where there is uncertainty about the propriety of an operation. It will also mean that the policy statements and auditing requirements apply whenever enforcement officers seek to covertly obtain information from members of the public. In our view, that is appropriate, as all such activities have the potential to intrude on reasonable expectations of privacy.
- 15.96 We suggest “covert operation” could be defined as an operation in which an enforcement officer or another person acting at the direction of an enforcement agency establishes, maintains or uses a relationship with any other person for the covert purpose of obtaining information or providing another person with access to information. This definition is based on the United Kingdom provisions addressing the use of “covert human intelligence sources”.¹³⁴ We would expect it to include any situation in which an agent interacts with another person in an attempt to obtain access to information on the basis of deception. We have, however, had limited time to test this definition. Some refinement of it may be appropriate as any amendment legislation is developed.

130 Our use of the term “unlawful activity” in this context excludes any potential breach of the New Zealand Bill of Rights Act 1990.

131 See Chapter 4 at paragraphs [4.23]–[4.24].

132 Under s 30 of the Evidence Act 2006, one of the factors to be taken into account in determining whether to exclude improperly obtained evidence is whether the impropriety was deliberate, reckless or done in bad faith (s 30(3)(b)).

133 See paragraphs [15.125]–[15.139].

134 Regulation of Investigatory Powers Act 2000 (UK), s 26(7)–(8).

- 15.97 Importantly, the definition we suggest is not limited to enforcement officers. We think it is appropriate that the protections applying to covert operations are engaged whenever the operation is instigated or directed by an enforcement agency, even if the agent is not an enforcement officer. In such cases the State is still, in effect, intruding on the privacy of individuals. We would not, however, consider the definition to be engaged where a private individual takes it upon themselves to obtain information covertly and provide it to an enforcement agency, without being under the agency's direction or control.
- 15.98 The definition also does not distinguish between relationships formed in person or online (for example, through Internet forums or chat rooms). We recognise that the relationships formed through online covert operations may not be as close or trusting as those formed during long-term in-person covert operations. The agent also will not enter private homes and any risks to their safety are likely to be much lower. However, we do not consider that online operations should, as a general rule, be treated differently. Like in-person operations, the risks and level of intrusiveness involved in a particular online operation will depend on the circumstances. Online operations have the potential to be as intrusive as in-person covert operations,¹³⁵ and could equally be used to elicit confessions from suspects.
- 15.99 We note that the warrant regime we discuss here will mainly be relevant to a small group of enforcement agencies that conduct covert operations at the more serious end of the spectrum, which may involve unlawful activity by agents or significant privacy intrusions. As we understand it, those agencies are currently Police, DIA, Customs and MPI¹³⁶ (although, as we discuss further below, the warrant regime may have limited relevance to MPI since its agents only commit regulatory offences for which they already have extensive immunities¹³⁷). As we have discussed, other regulatory agencies such as Inland Revenue undertake activity as part of their day-to-day operations that would be captured by the definition of "covert operations" we suggest. We would not expect those kinds of activities to engage the warrant regime. Similarly, much of the lower-level activity of Police, DIA, Customs and MPI that meets the definition would not be done pursuant to a warrant. The recommendations we make below in relation to policy statements and external audits would apply in these instances.

Who should issue covert operations warrants?

- 15.100 Authorisation of investigatory activity can occur through external approval (for example, a judicial warrant) or internal approval (for example, authorisation by a senior member of an enforcement agency). In the Search and Surveillance Act, internal approval is not generally favoured. The existing warrants and orders in the Act must be issued by judges or (in some cases) other issuing officers.
- 15.101 Some enforcement agencies told us that, if an authorisation regime is considered desirable for covert operations, internal authorisation would be their preference. This was largely due to the fact that covert operations are unpredictable. Since they involve interaction with targets, they cannot be controlled to the same degree as other enforcement activity (such as the execution of a search warrant or surveillance warrant). Enforcement agencies were concerned that if warrants were issued by judges, there would need to be constant communication with the judge as the operation develops to ensure the warrant continues to cover the planned activity.

135 See paragraph [15.24]. Many of the factors discussed there that might lead to a covert operation being considered a "search" for the purposes of s 21 of the New Zealand Bill of Rights Act 1990 could apply equally to online covert operations. For example, a close and trusting relationship may be formed with a target over a long period of time, and they may be deceived into disclosing highly personal information that they would not otherwise choose to disclose.

136 Other agencies may seek to extend their capability in this area in future. For example, as we discussed in Chapter 8 at paragraph [8.61], Immigration New Zealand conducts investigations into serious offending that could potentially benefit from the use of covert methods.

137 See paragraph [15.143].

- 15.102 We appreciate that covert operations are different from other warranted activity. However, in our view, those differences can be managed through a sufficiently flexible warrant regime.¹³⁸ We consider internal authorisation by a senior member of an enforcement agency is unlikely to provide a significant benefit over the current, informal arrangements. Enforcement officers—even those not directly involved in a particular investigation—cannot, by virtue of their position, be expected to impartially assess where the appropriate balance lies between law enforcement and human rights values. If an operation involves a sufficiently high level of risk¹³⁹ or intrusion that authorisation is desirable, that authorisation should be sought from an independent and impartial person.
- 15.103 Our preference is for covert operations warrants to be issued by High Court judges, bearing in mind the sensitive methods involved and the difficult questions that may arise concerning individuals' rights. However, we did not have the opportunity during this review to adequately consult the judiciary on this proposal. Because of this, we do not make a firm recommendation about who should issue warrants, provided they are independent, have the necessary legal expertise and are sufficiently resourced and trained to deal with highly confidential operational information. As an alternative to High Court judges, an independent commissioner could be appointed to issue warrants (such as a former judge or other person with significant legal experience). This would be similar to the approach taken to warrants issued to intelligence agencies under the Intelligence and Security Act 2017.¹⁴⁰
- 15.104 We acknowledge the judiciary may have concerns about authorising covert operations, given their unpredictability and the fact that they may involve acts by agents that would otherwise amount to a criminal offence. Our preliminary view is that neither of these considerations presents a barrier to warrants being issued by judges. We briefly explain why, to assist the government in deciding what approach should be taken.
- 15.105 First, warrants frequently authorise conduct that would otherwise be unlawful. Judges already issue warrants authorising interception, which would otherwise amount to an offence under the Crimes Act 1961.¹⁴¹ Concerns may legitimately arise if the offences that can be authorised are not constrained, so that judges are required to determine the extent to which a particular type of offending can potentially be justified for law enforcement purposes. However, that can be avoided by including sufficiently clear immunity provisions in the Act.¹⁴²
- 15.106 The seriousness of the potential criminal conduct involved is, in our view, all the more reason to provide for judicial authorisation as a safeguard. In *Grollo v Palmer*, the High Court of Australia was asked to declare unconstitutional the provisions in the Telecommunications (Interception) Act 1979 that empower eligible judges to issue interception warrants. The applicant argued that the power to issue interception warrants was incompatible with judicial functions and contrary to the separation of powers. The declaration was refused. In their joint majority judgment, Brennan CJ, Deane, Dawson and Toohey JJ said:¹⁴³
- ... it is precisely because of the intrusive and clandestine nature of interception warrants and the necessity to use them in today's continuing battle against serious crime that some impartial authority, accustomed to the dispassionate assessment of evidence and sensitive to the common law's protection of privacy (see *Haisman v Smelcher* [1953] VLR 625 at 627) and property (both real and

138 See paragraphs [15.114]–[15.115], [15.119]–[15.120] and [15.123]–[15.124].

139 As discussed in paragraphs [15.60]–[15.65].

140 Intelligence warrants relating to New Zealanders are issued by Commissioners of Intelligence Warrants jointly with the responsible Minister (Intelligence and Security Act 2017, s 57). Commissioners must have previously held office as a High Court judge (s 113).

141 Crimes Act 1961, s 216B.

142 As we discuss below at paragraphs [15.140]–[15.145].

143 *Grollo v Palmer* [1995] HCA 26, [1995] 4 LRC 63 at 80.

personal), be authorised to control the official interception of communications. In other words, the professional experience and cast of mind of a judge is a desirable guarantee that the appropriate balance will be kept between the law enforcement agencies on the one hand and criminal suspects or suspected sources of information about crime on the other.

In other countries the same view has been taken of the desirability, if not the necessity, for judicial issuing of a warrant to authorise secret surveillance of suspects in criminal cases. In such cases, the European Court of Human Rights said in *Klass v Federal Republic of Germany* (1978) 2 EHRR 214 at 235:

‘The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.’

While these observations were made in the context of interception, we consider that they are equally applicable to covert operations, which can be similarly “intrusive and clandestine”.

15.107 Second, in terms of the unpredictability of covert operations, applications for warrants would need to set out the parameters of the operation in sufficient detail to enable the judge to understand what authorisation is being sought for and to assess whether the statutory criteria are met. If circumstances change significantly after the warrant is issued, a variation would need to be sought. Judges would not be expected to approve applications that are vague or overly broad.

15.108 Again, comparisons can be drawn with the existing surveillance warrant provisions. Surveillance is similarly forward-looking and operations may evolve in unexpected ways (although perhaps not to the same extent as covert operations). Under the Act, surveillance can be authorised by a judge even where it is not possible to identify the person, place, vehicle or other thing that is the object of the surveillance or the evidential material that may be obtained. Instead, it is sufficient if the warrant identifies the circumstances in which the surveillance will be undertaken in enough detail to identify the parameters of, and the objectives to be achieved by, the surveillance.¹⁴⁴ We are not aware of judges experiencing any problems in the application of these provisions.

Grounds for issuing warrants

15.109 In order to issue a covert operations warrant, the judge or commissioner would need to be satisfied that there are reasonable grounds:

- to suspect an offence punishable by imprisonment has been, is being or will be committed; and
- to believe that the operation will obtain evidential material relating to that offence.

These grounds are equivalent to those for issuing search warrants and surveillance device warrants.

15.110 The judge or commissioner would also need to take into account the principles we have recommended including in the Act. For example, they would need to consider whether the intrusion on privacy involved in the proposed operation is proportionate to the public interest in the investigation and prosecution of the offence; and whether the proposed operation minimises the degree of intrusion on privacy so far as possible in the circumstances. The judge or commissioner would have discretion whether to issue the warrant even if the grounds are

144 Section 55(4).

met. So, for instance, they could decline to issue a warrant if they consider the offence under investigation is insufficiently serious to justify the intrusiveness of the proposed operation.

- 15.111 In addition, in light of the particular concerns that arise in relation to covert operations, the Act should provide that a warrant must not be issued if the proposed operation is likely to seriously endanger the health or safety of any person or result in serious loss of or damage to property (other than property owned by the enforcement agency or unlawful goods such as illicit drugs). In our view, the public interest in law enforcement is unlikely to justify State involvement in such conduct.
- 15.112 We recognise that there will always be some level of risk involved in covert operations, particularly to the safety of the agent. That should not prevent an operation from proceeding where appropriate safeguards can be put in place. “Seriously endanger” is intended to be a reasonably high bar. We consider it unlikely that enforcement agencies would ever seek a warrant where such a high level of risk exists, or that a judge or commissioner would approve it, but the Act should remove any doubt. Similar limitations exist in the Australian legislation.¹⁴⁵
- 15.113 We acknowledge that including a “reasonable grounds” threshold for issuing covert operations warrants may prevent warrants from being sought or issued for operations aimed at intelligence-gathering or crime detection. In such cases, there may not yet be reasonable grounds to suspect the commission of a particular offence or to believe evidential material will be obtained. In accordance with the recommendations we make below, any such operations would still be subject to a policy statement and external audits. We considered it inappropriate to enable warrants to be issued before the point at which specific offending is being investigated, given that warrants will enable recourse to immunities under the Act and may permit highly intrusive operations. In general, powers that will involve the commission of offences or significant intrusions on reasonable expectations of privacy should only be permitted where the “reasonable grounds” threshold is satisfied¹⁴⁶ (although there are some exceptions to this, as we discuss below).¹⁴⁷
- 15.114 We do not recommend that an offence threshold be imposed for covert operations warrants. The warrants should be available, in theory, in relation to any imprisonable offence. Offence thresholds do exist in the Australian legislation: a “controlled operation” can only be authorised in relation to specified offences punishable by three years’ imprisonment or more.¹⁴⁸ However, the Australian regime is limited to operations that may involve the commission of an offence.¹⁴⁹ The United Kingdom regime, which is not limited to where offences will be committed, contains no offence threshold.¹⁵⁰
- 15.115 As we have said, we propose a broad definition of “covert operations” so that warrants can be sought by enforcement agencies before carrying out potentially intrusive operations even if they will not involve the commission of offences. Given the wide variation between different covert operations and the level of intrusion they involve, any offence threshold would be arbitrary. The better approach, in our view, is for the judge or commissioner to consider whether the proposed activity is proportionate to the interest in law enforcement having regard to the

145 See, for example, Crimes Act 1914 (Cth), s 15GI; Crimes (Controlled Operations) Act 2004 (Vic), s 131F; Law Enforcement (Controlled Operations) Act 1997 (NSW), s 7.

146 See, for example, Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [3.9]–[3.10]; *Legislation Advisory Committee Guidelines on Process and Content of Legislation* (Wellington, 2014) at [18.3]. This is in contrast to our recommendations in relation to declaratory orders, which can only apply to lawful activity.

147 See paragraph [15.143].

148 Crimes Act 1914 (Cth), ss 15GE and 15GI.

149 Crimes Act 1914 (Cth), s 15GD.

150 Regulation of Investigatory Powers Act 2000 (UK), s 29.

particular circumstances of each case.¹⁵¹ We envisage that serious offending would need to be under investigation to justify any operation that is likely to involve significant intrusions on privacy; the commission of offences by agents; the potential for infringing NZBORA rights (such as where a confession is sought); and/or the application of substantial resources by the State.

15.116 The Act should make it clear that a covert operations warrant cannot authorise activity that requires a surveillance warrant. For example, if an undercover officer wishes to carry out interception (in circumstances where none of the exceptions to the warrant requirement apply)¹⁵² a surveillance warrant would need to be obtained in addition to the covert operations warrant – although this could be done at the same time.

15.117 This is important to ensure that covert operations warrants are not used to circumvent the special protections applying to some types of surveillance. For example, surveillance warrants permitting interception or visual trespass surveillance can only be issued in relation to specified serious offences,¹⁵³ and only to constables or enforcement officers of approved agencies.¹⁵⁴ Parliament's recognition that these types of surveillance should be subject to stricter controls would be undermined if covert operations warrants (which would not be subject to these requirements) could permit their use.

Content of applications and warrants

15.118 Warrant applications would need to include the following information:

- The name of the applicant.
- The suspected offence in relation to which the warrant is sought.
- A description of the evidential material believed to be able to be obtained through the operation.
- The name or other description (such as a code name) of the agent(s) who it is proposed will conduct the operation. If the agent is not an enforcement officer, this should be made clear and the application should provide any information available to help the issuing officer assess the agent's integrity and reliability.
- The period for which the warrant is sought, up to a maximum of three months.
- The name, address or other description of the target(s).
- A description of the activity it is proposed the agent will carry out. This would include details such as the agent's proposed cover story, how they intend to approach the target and/or gain the target's trust, and how they will seek to obtain the evidential material sought. For example, any "scenarios" that are planned would need to be described. The applicant should also signal any potentially unlawful activity they anticipate the agent may need to carry out.

15.119 If it is not possible to provide sufficient information to identify the target or describe the evidential material to be obtained, the application could instead state the circumstances in which the covert operation is intended to be carried out in enough detail to identify the parameters of, and the objectives to be achieved by, the operation. This is similar to the current

151 In accordance with the principle we have recommended in Chapter 4 (see paragraphs [4.44]–[4.56]).

152 Search and Surveillance Act 2012, s 47 and Chapter 9 at paragraph [9.19].

153 Section 45.

154 Section 49(5).

requirements for surveillance device warrants.¹⁵⁵ It will help to ensure the warrant regime is sufficiently flexible in light of the forward-looking nature of covert operations.

- 15.120 Although applications should, where possible, identify the target(s) of an operation, agents would not be prevented from engaging with other people not specified as targets. That will be unavoidable in many covert operations. However, if the circumstances or the scope of the operation change significantly, the applicant would need to report back to the judge or commissioner and seek variation of the warrant. This might be the case, for example, if the agent identifies a new suspect and wishes to pursue them as a target, or if the planned activity has not been successful and the agent wishes to try a new approach that is substantially different to what is described in the warrant.
- 15.121 We consider three months is an appropriate maximum period of validity for warrants, but the Act should permit renewal. After three months it is likely that the circumstances will have changed so it is appropriate that the situation be reviewed by the judge or commissioner if the operation is to continue.
- 15.122 When issuing a warrant, the judge or commissioner should be expressly permitted to impose any conditions they consider reasonable.

Other issues relating to warrants

- 15.123 As we have recommended in relation to declaratory orders, sections 98(2), 99, 100, 101 and 105 of the Act should apply to covert operations warrants with any necessary modifications.¹⁵⁶ These sections set out general requirements and procedures that apply to warrants, including allowing for electronic or oral applications in appropriate cases. An ability to seek an oral variation of a warrant may be particularly valuable in the case of covert operations, given the potential for them to develop in unexpected ways.
- 15.124 There may also be merit in permitting operations that may involve unlawful activity to be commenced or varied without a warrant in specified situations of urgency or emergency. The warrantless surveillance provisions could provide a model for this.¹⁵⁷ Any such warrantless power should only be valid for a short period of time—such as 48 hours—to enable a warrant to be obtained. We do not make any recommendations about a warrantless covert operations power as we have not had the opportunity during this review to give it proper consideration. However, we suggest this issue be addressed during the development of any amendment legislation.

155 Section 49(2).

156 Chapter 6 at paragraph [6.82].

157 Section 48.

RECOMMENDATIONS

- R54 A provision should be inserted into the Act to permit an enforcement officer to apply for a warrant to conduct a covert operation.
- R55 "Covert operation" should be defined as an operation in which an enforcement officer or another person acting at the direction of an enforcement agency establishes, maintains or uses a relationship with any other person for the covert purpose of obtaining information or providing another person with access to information.
- R56 The Act should provide that covert operations warrants should:
- (a) Be issued by an independent, impartial and legally-qualified person who can be trusted with sensitive operational information. This role could be performed by High Court judges (subject to consultation with the judiciary) or a commissioner appointed under the Act.
 - (b) Only be issued where there are reasonable grounds to suspect an offence punishable by imprisonment has been, is being or will be committed; and to believe that the operation will obtain evidential material relating to that offence.
 - (c) Not be issued if the operation is likely to seriously endanger the health or safety of any person or result in serious loss of or damage to property (other than property owned by the enforcement agency or unlawful goods).
 - (d) Be capable of being renewed and varied.
 - (e) Be subject to any conditions that the issuing officer considers reasonable.
- R57 The Act should state that covert operations warrants cannot authorise activity for which a surveillance warrant is required.
- R58 Applications for covert operations warrants should include the following information:
- (a) the name of the applicant;
 - (b) the suspected offence in relation to which the warrant is sought or issued;
 - (c) a description of the evidential material believed to be able to be obtained through the operation;
 - (d) the name or other description (such as a code name) of the agent(s) who it is proposed will conduct the operation;
 - (e) the period for which the warrant is sought, up to a maximum of three months;
 - (f) the name, address or other description of the target(s);
 - (g) a description of the activity it is proposed the agent will carry out; and
 - (h) the circumstances in which the covert operation is intended to be carried out in enough detail to identify the parameters of, and the objectives to be achieved by, the operation, if it is not possible to provide sufficient information to identify the target or describe the evidential material to be obtained.
- R59 Sections 98(2) (relating to requirements for further information), 99 (application must be verified), 100 (mode of application for a search warrant), 101 (retention of documents) and 105 (transmission of search warrant) should apply to covert operations warrants, with any necessary modifications.

POLICY STATEMENTS

- 15.125 Covert operations warrants will not cover all covert operations. As we have said, some activity that would fall within the definition of “covert operations” will be relatively unintrusive and form part of day-to-day enforcement activity. However, we consider that whenever an agency interacts with targets using deception in order to obtain information, there is potential for NZBORA rights to be affected. Although requiring a warrant in all such cases would be unworkable, enhanced transparency and accountability is desirable to help ensure that covert operations are only used in appropriate circumstances and are conducted in a reasonable manner.
- 15.126 We therefore recommend that all agencies that conduct covert operations should be required to publish a policy statement.¹⁵⁸ These statements should include guidance on:
- Relevant considerations that should be taken into account when deciding whether to initiate a covert operation and how it should be conducted. This should include guidance on how the principles in the Act and any relevant case law might apply to the types of covert operations conducted by the agency. It may also direct consideration of factors such as the cost of an operation and the level of risk to the safety of agents.
 - The situations in which a covert operations warrant should be sought.
 - Any matters that should be specifically highlighted in warrant applications.
 - Internal planning, approval, monitoring, reporting, record-keeping and evaluation requirements. For example, an operational plan may need to be approved at a senior level before complex operations are commenced, and/or dedicated staff members may need to be allocated to liaise with the agent and ensure that accurate records are kept.
 - Arrangements to protect the safety of agents and others.
 - What processes will be followed if any potential misconduct by agents or other enforcement officers is identified.
- 15.127 We understand Police, MPI, DIA and Customs already have internal policies on the use of covert operations. These policies are usually kept confidential because they contain information about the methods used by enforcement agencies that could prejudice investigations. Police indicated it could publish a policy statement on covert operations provided the statements would not be required to disclose operationally sensitive information. DIA, Customs and Inland Revenue also did not oppose this idea, although they also did not necessarily see a need for such a requirement. MPI opposed being required to publish a policy statement, although it did prefer this option to a requirement to obtain authorisation.
- 15.128 Policy statements would not need to include any information that there would be grounds for withholding under the Official Information Act 1982.¹⁵⁹ The information listed above primarily relates to processes and general considerations. It should be able to be framed in a way that is useful without disclosing sensitive information. We note that some law enforcement agencies overseas publish detailed policies on the use of covert operations.¹⁶⁰ Agencies may, of course, still choose to have more detailed internal guidance that does include sensitive information.

158 The general purpose and effect of policy statements is discussed in Chapter 5.

159 Official Information Act 1982, ss 6 and 9.

160 See, for example, Council of the Inspectors-General on Integrity and Efficiency *Guidelines on Undercover Operations* (United States, 2013); Home Office *Covert Human Intelligence Sources: Code of Practice* (United Kingdom, 2014).

RECOMMENDATION

- R60 The Act should require policy statements to be issued in respect of covert operations. Covert operations policy statements should contain guidance on:
- (a) considerations that should be taken into account when deciding whether to initiate a covert operation and how it should be conducted;
 - (b) the situations in which a covert operations warrant should be sought;
 - (c) any matters that should be specifically highlighted in warrant applications;
 - (d) internal planning, approval, monitoring, reporting, record-keeping and evaluation requirements;
 - (e) the processes that will be followed if any potential misconduct by agents or other enforcement officers is identified; and
 - (f) arrangements to protect the safety of agents and others.

EXTERNAL AUDITS

- 15.129 Covert operations are necessarily carried out in secret. Targets and other people who are affected cannot realistically be notified without prejudicing investigations. This means that, unless the information obtained is relied on in a subsequent prosecution, there is little opportunity for complaints to be made or proceedings brought if misconduct occurs. Because covert operations may be used at an early stage in an investigation—and the information obtained may form the basis of warrant applications rather than being directly relied on in prosecutions—they are also less likely to be considered by a court in the context of admissibility contests than surveillance operations or searches.
- 15.130 In addition, although we have recommended that agencies that conduct covert operations be required to publish policy statements on their use, we recognise those statements may not provide a high level of detail. While policy statements should include as much relevant information as possible, we expect some information will be omitted to avoid prejudicing investigations.
- 15.131 We consider that, in light of these unique aspects of covert operations, there is a particular need for external oversight. We think this can be achieved through independent auditing of covert operations. This will help to identify any instances where operations are carried out in an unreasonable manner or do not comply with the requirements in the Act or the applicable policy statement. Steps can then be taken to reduce the likelihood of mistakes being made in future. This additional safeguard is, in our view, necessary to uphold the rule of law and to ensure an appropriate balance is maintained between law enforcement and the protection of individuals' rights.
- 15.132 Where surveillance is carried out, enforcement officers are required to report back to a judge. The judge may order destruction of evidence or notification of the target. We considered whether a similar approach could be taken for covert operations, but concluded it would be unsuitable. Unlike surveillance, for which a warrant or power is specifically required, many covert operations will not occur under a specific warrant or warrantless power. Confining oversight to warranted covert operations would be insufficient to address the risks associated with them, but reporting to a judge on all covert operations would be unrealistic.

- 15.133 Instead, we recommend that all warranted covert operations and a selection of non-warranted covert operations should be subject to annual auditing by an external person or body. The aim of the audit would be to assess whether the operations complied with the applicable policy statement and (where relevant) warrants, and to identify any instances of potentially unlawful or unreasonable conduct.
- 15.134 Police supported auditing of covert operations, although its preference would be for an internal audit. DIA supported independent auditing of warranted covert operations but not of unwarranted ones, due to the resourcing impact that would have. Customs only supported external auditing in place of a warrant, for operations that may need to rely on immunities under the Act. Inland Revenue opposed external auditing due to concerns that divulging their methodology might prejudice their investigations and could conflict with the tax secrecy rules in the Tax Administration Act 1994. MPI also opposed external auditing.
- 15.135 We consider DIA's concern about the resourcing impact of auditing non-warranted covert operations can be addressed by only requiring a selection of such operations to be audited. Because of the wide definition of "covert operations" we have recommended, requiring audits of every operation falling within its scope would create an undue burden both on the auditor and on the agencies being audited. However, agencies would need to keep sufficient records of all covert operations to ensure that they can be audited if required.
- 15.136 We do not think the Act should be prescriptive about how the auditor should select which non-warranted covert operations are audited or how many. This will depend on the agency concerned and the type of operations they carry out. Over time the auditor will gain a sense of the type of operations that may raise concerns, and may choose to focus their efforts accordingly (although a certain amount of random auditing is also likely to be beneficial).
- 15.137 We do not express a view on which person or body should perform this auditing function. Options include the Independent Police Conduct Authority (IPCA), an Ombudsman or a person appointed under statute specifically for that purpose. The auditor should have broad powers to access operational information.¹⁶¹ They would therefore need to be capable of maintaining the confidentiality of operationally sensitive records.
- 15.138 We note that the IPCA already has relevant expertise in reviewing law enforcement conduct. However, conferring an auditing function on it would significantly expand its role, since the audits would need to be carried out in respect of other enforcement agencies in addition to Police.
- 15.139 The auditor should report to the House of Representatives annually on the outcome of the audit. In addition, where any potential misconduct or irregularities are detected, the case should be referred to the IPCA, in the case of Police (unless IPCA is the auditor), or to the responsible Minister, in the case of other enforcement agencies. The auditor's report could include recommendations for the IPCA or Minister's consideration (for example, that an affected person be notified of the operation or that material obtained during the operation be destroyed). The IPCA or the Minister could then initiate an investigation if that is considered necessary. The IPCA could make recommendations to the Commissioner of Police in the ordinary way,¹⁶² or the Minister could direct the relevant enforcement agency to take steps to address any problems identified.

161 Section 179 of the Intelligence and Security Act 2017 (relating to the powers of the Inspector-General of Intelligence and Security) provides a useful comparison.

162 Independent Police Conduct Authority Act 1988, s 27.

RECOMMENDATION

- R61 The Act should be amended to provide that all warranted covert operations and a selection of non-warranted covert operations should be subject to annual auditing by an external person or body. The auditor should:
- (a) assess whether an operation complied with the applicable policy statement and (where relevant) warrant, and identify any instances of potentially unlawful or unreasonable conduct;
 - (b) have broad powers to access any relevant operational information;
 - (c) report to the House of Representatives annually on the outcome of the audit; and
 - (d) refer any case involving a potential irregularity to the Independent Police Conduct Authority, in the case of Police, or to the responsible Minister, in the case of other enforcement agencies.

IMMUNITIES

- 15.140 The statutory immunities currently available to some agencies that conduct covert operations are incomplete. Police and DIA gave a number of examples where agents may be unable to carry out a covert operation effectively without risking the commission of offences for which they currently have no statutory immunity.¹⁶³ While prosecutorial discretion may be exercised, that provides little certainty for enforcement officers and little transparency for the public. We consider it is preferable, where possible, to have clear statutory immunities. This will allow Parliament to determine—with the benefit of public consultation—what offences agents may be justified in committing.
- 15.141 We recommend the Act should provide that any person is immune from civil liability and from criminal liability *for the commission of specified offences* for any act done in good faith in relation to the execution of a covert operations warrant, provided the execution is carried out in a reasonable manner. The Ministry of Justice will need to work with enforcement agencies that conduct covert operations to determine which offences the immunities should apply to. However, we would envisage they could include offences such as participation in an organised criminal group, receiving stolen property and deception offences (such as forgery). They should not include any violent or sexual offending.
- 15.142 Section 167 of the Act provides that where any person is immune from liability under the existing immunity provisions in the Act, the Crown is also immune from civil liability in tort in respect of that person's conduct. That section should also apply to the new immunity. This would not prevent other claims against the Crown, such as claims for public law damages in respect of breaches of NZBORA.¹⁶⁴
- 15.143 Consideration should also be given to whether any of the existing immunities available to agencies under other legislation should be consolidated into the covert operations immunity in the Act. This would mean that a covert operations warrant would be required in order to engage the immunity for those offences. That may be appropriate, for example, for some of the more serious offences under the Misuse of Drugs Act 1975 (such as supply or production offences). We do not envisage this would be appropriate for all—or even most—of the existing

163 See paragraphs [15.76]–[15.77].

164 *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA).

immunities. For example, it is unlikely to be practicable or necessary to require a warrant to engage the following immunities:

- the immunities that protect regulatory enforcement officers such as fisheries officers and park rangers from liability for regulatory offences;
- the provisions that allow minors to carry out controlled purchases of alcohol at the request of Police;¹⁶⁵
- the provisions that allow Police, Customs and DIA staff to possess objectionable publications.¹⁶⁶

15.144 Restricting the immunity to specified offences contrasts with the approach to existing immunities in the Act. Where a search or surveillance warrant is issued, immunities apply in respect of criminal liability generally.¹⁶⁷ However, the potential scope of search and surveillance warrants is more constrained than will be the case for covert operations warrants. For example, the acts an enforcement officer could carry out in good faith in relation to the execution of a surveillance warrant are likely to be limited to reasonably obvious offences such as using an interception device.¹⁶⁸

15.145 By contrast, an agent conducting a covert operation could potentially engage in a wide variety of offences in order to establish or maintain a cover identity, depending on the context. Unless the immunity is confined to specific offences, the person responsible for issuing the warrant would be required to determine—with no statutory guidance—what offences can reasonably be committed for the purpose of executing a covert operations warrant. We think that is a policy issue more appropriately determined by Parliament.

RECOMMENDATIONS

- R62 A provision should be inserted into the Act stating that any person is immune from civil liability and from criminal liability for the commission of specified offences for any act done in good faith in relation to the execution of a covert operations warrant, provided the execution is carried out in a reasonable manner.
- R63 Section 167 (immunity of the Crown) should be amended (if required) to apply to the new immunity in respect of covert operations warrants.

ASSUMED IDENTITY INFORMATION

15.146 As we have explained above, there is no comprehensive regime for enforcement agencies to obtain and use assumed identity information for cover purposes.¹⁶⁹ The current provisions are scattered throughout different statutes and do not apply to all information that may assist in creating cover for agents. Notably, passports are not covered, nor is there any provision for the creation of corporate identities.

15.147 Until recently, the New Zealand Security and Intelligence Service and Government Communications Security Bureau were in a similar position. When the legislation governing those agencies was reviewed in 2016, the reviewers recommended the introduction of a

165 Sale and Supply of Alcohol Act 2012, ss 243(2) and 244(4)(c).

166 Films, Videos, and Publications Classification Act 1993, s 131(4).

167 Search and Surveillance Act 2012, s 165.

168 Crimes Act 1961, s 216B.

169 See paragraphs [15.38]–[15.39].

statutory regime permitting the agencies to obtain, create and use any identification information necessary for cover purposes.¹⁷⁰ The reviewers also observed:¹⁷¹

In addition to the NZSIS and GCSB, there are a range of other government agencies (such as Police) that may need to conduct undercover operations. While it is outside the scope of this review, the government may wish to consider whether any other legislative amendments are required to enable this.

- 15.148 As a result of the reviewers' recommendations, Part 3 of the Intelligence and Security Act 2017 now provides a regime for the creation of assumed identities and corporate identities. The regime includes immunities for people authorised to use assumed identities and anyone assisting the agencies to make false documents or to create or maintain corporate identities.¹⁷² The Director-General of each agency is required to keep a register of assumed identities and legal entities created or maintained, which can be accessed by the responsible Minister and the Inspector-General of Intelligence and Security.¹⁷³ In addition, the responsible Minister is required to issue a policy statement providing guidance on the acquisition, use and maintenance of assumed identities.¹⁷⁴
- 15.149 We recommend that the Search and Surveillance Act be amended to include an assumed identity regime similar to that contained in the Intelligence and Security Act. The regime would apply in full to Police. The Ministry of Justice should consult other agencies that conduct covert operations (such as MPI, DIA and Customs) to determine whether the regime should apply in whole or part to their officers as well.
- 15.150 The regime would allow specified enforcement officers to obtain and use any records necessary to create or maintain assumed identities and corporate identities. The enforcement officer and any person assisting them in the creation of records (such as employees of government agencies and financial institutions) would have immunity from any associated civil or criminal liability. A register of assumed identities would need to be maintained by the Commissioner of Police and be made available for review by the IPCA.

RECOMMENDATION

R64 The Act should be amended to include an assumed identity regime for Police similar to that contained in the Intelligence and Security Act 2017. The Ministry of Justice should consult other agencies that conduct covert operations to determine whether the regime should apply to their officers in whole or part.

170 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) at [6.114]–[6.115].

171 At [6.119].

172 Intelligence and Security Act 2017, ss 31–32 and 42–44.

173 Intelligence and Security Act 2017, s 45.

174 Intelligence and Security Act 2017, s 206(b).

Chapter 16

Examination orders

INTRODUCTION

16.1 In our Issues Paper, we described the existing examination order regime in the Search and Surveillance Act 2012 (the Act) and asked submitters whether it should be retained. In this chapter, we explain our conclusion that the regime should remain in the Act.

BACKGROUND

The statutory scheme

16.2 The examination order regime in the Act provides a power—available only to New Zealand Police—to obtain an order from a judge¹ requiring a person (the examinee) to appear and answer questions in relation to identified information, where the examinee has previously refused to do so.²

16.3 An examination order may be made in either a “business” or “non-business” context. Those terms are defined in section 3.³ 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 they do not wish to disclose.

16.4 In our Issues Paper, we described the various procedural and substantive hurdles that need to be overcome before Police can obtain an examination order:⁴

- The application can 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.⁵
- The Commissioner of Police or a delegate of the Commissioner must conduct the examination⁶ and provide a formal report to the issuing judge within one month.⁷
- Examination orders are available only where there are reasonable grounds to suspect an offence has been, is being, or will be committed;⁸ there are reasonable grounds to believe the examinee has information that constitutes evidential material in respect of the offence;⁹ and

1 Section 3 of the Search and Surveillance Act 2012 defines “Judge” as a District Court judge or a judge of the High Court.

2 Search and Surveillance Act 2012, ss 33–43.

3 “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.

4 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [10.7]–[10.11] [Issues Paper].

5 Search and Surveillance Act 2012, ss 33(1) and 35(1).

6 Section 39(1).

7 Section 43.

8 Sections 34(a) and 36(a).

9 Sections 34(b) and 36(b).

where the examinee has been given a reasonable opportunity to provide the information and has declined to do so.¹⁰

- Examination orders may only be made in relation to sufficiently serious offences. In a business context, they may only be made if the offence in question is punishable by five years' imprisonment or more.¹¹ 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.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

16.5 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-incrimination¹⁵ or any other privilege recognised under the Act.¹⁶

16.6 As we explained in our Issues Paper,¹⁷ examination orders under the Act were an entirely new power for Police in the investigation of suspected criminal offending.¹⁸ The rationale for introducing an examination order regime into the Act was that:

- it could help Police unravel complex transactions and arrangements when investigating serious financial crime and organised crime;¹⁹ and
- compulsory questioning could assist in situations where a person was reluctant to co-operate with Police on the grounds of professional confidentiality, by allowing such persons to assist Police without fear of adverse consequences.²⁰

16.7 However, the concept and use of examination orders was not novel. There are similar powers in other statutes that permit the State to submit people to compulsory questioning. We described three examples in our Issues Paper: the Serious Fraud Office Act 1990;²¹ the Insolvency Act

10 Sections 34(d) and 36(d).

11 Section 34(a).

12 Section 36(a). The definition of "organised criminal group" in s 98A(2) of the Crimes Act 1961 applies to this section.

13 Section 38(b).

14 Section 40.

15 Section 138(1).

16 Section 139(1). 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: ss 138(3) and 139(2). It is an offence to fail to comply with an examination order without reasonable excuse: s 173. 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).

17 Issues Paper, above n 4, at [10.25].

18 We also explained that examination orders were not considered by the Law Commission in *Search and Surveillance Powers* (NZLC R97, 2007), as they were beyond the Commission's terms of reference. The regime was developed at a later point, when 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, including SFO's ability to require persons to submit to compulsory questioning. Accordingly, a Police-only examination order was included in the Search and Surveillance Powers Bill 2008 (300-1), introduced by the Labour Government in September 2008. 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).

19 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [164].

20 Search and Surveillance Bill 2009 (45-2) (select committee report) at 8–9; Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [170]. In the case of persons who have obtained information about suspected offending in a non-business context, there are also many reasons why a person may be reluctant to disclose that information to Police voluntarily: Search and Surveillance Bill 2009 (45-2) (select committee report) at 9.

21 The Director of SFO can require persons to answer questions in the investigation of suspected serious or complex fraud: s 9 of the Serious Fraud Office Act 1990.

2006;²² and the Criminal Proceeds (Recovery) Act 2009.²³ Those regimes do not preclude questions that may elicit self-incriminating answers,²⁴ although there are restrictions on the ability to use self-incriminating statements obtained during the examination process in criminal proceedings.²⁵ Furthermore, the examination power under the Serious Fraud Office Act can be exercised by the Director giving notice in writing to the examinee, rather than requiring a judicial order.²⁶

Legislative history

- 16.8 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.²⁷
- 16.9 The Select Committee acknowledged submitters' concerns that examination orders would remove an individual's right to silence, but concluded there were strong policy reasons for having an examination order regime.²⁸ 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 (as examination orders would require prior judicial authorisation).²⁹

CONSULTATION

Issues Paper

- 16.10 The examination order regime has yet to be employed by Police.³⁰ We were told that the regime has not been used because of knowledge gaps within the police force about their availability; and also because Police does not tend to investigate many serious or complex fraud cases (most being conducted by the Serious Fraud Office (SFO)).³¹
- 16.11 Given that examination orders have not been used, it has not been possible for us to assess the operation of the regime, as required by our terms of reference. Nevertheless, we sought submitters' views on whether the examination order regime should be retained. We noted that the lack of use of examination orders under the Act perhaps suggested there was no real

22 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: s 165(1).

23 Section 107 of the Criminal Proceeds (Recovery) Act 2009 empowers a judge to make an order requiring a person to attend before the Commissioner and 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.

24 Serious Fraud Office Act 1990, s 27; Insolvency Act 2006, s 184(2); Criminal Proceeds (Recovery) Act 2009, s 163.

25 Serious Fraud Office Act 1990, s 28(1); Insolvency Act 2006, s 185(2); Criminal Proceeds (Recovery) Act 2009, s 165.

26 Serious Fraud Office Act 1990, s 9(1).

27 Search and Surveillance Bill 2009 (45-2) (select committee report) at 8; and see the submissions referred to in Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [159]. As we explained in our Issues Paper, the "right to silence" has been described as a network of loosely linked rules or principles of immunity, differing in scope and rationale (*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). 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, in ss 23(4) and 25(d) of the New Zealand Bill of Rights Act 1990 and s 60 of the Evidence Act 2006). See Issues Paper, above n 4, at [10.21]–[10.22].

28 Search and Surveillance Bill 2009 (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.

29 Search and Surveillance Bill 2009 (45-2) (select committee report) at 9. 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, creating an internal oversight process for making applications, and strengthening reporting requirements.

30 According to Police annual reports (the latest report was for the year ending 30 June 2016), since 1 October 2012 no applications for examination orders have been made, granted or refused.

31 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.

practical need for them.³² We also observed that removal of the regime could create an anomaly in the powers available to Police and SFO when investigating similar offending.³³

- 16.12 We also asked whether the Act should be clearer about who can be an examinee. We expressed a very preliminary view that there was no policy justification for subjecting a person suspected of, arrested for, or charged with the offending in question to compulsory examination; and that there could be merit in expressly stating this in the Act.³⁴

Submissions

- 16.13 Most of the submitters who expressed a view on this issue supported the retention of the examination order regime. Although the regime has not yet been used, those submitters considered that examination orders could be a useful tool in the future when investigating serious complex offending. One submitter suggested it would be anomalous for examination powers to be available under the Serious Fraud Office Act, Insolvency Act and Criminal Proceeds (Recovery) Act but not the Search and Surveillance Act.
- 16.14 One submitter considered the availability of examination orders should be extended in a non-business context beyond serious and complex fraud and offending committed by an organised criminal group, to cover serious offending by an individual that could have major national and international consequences. For example, the submitter suggested an examination power could have assisted in relation to Operation Concord – a significant investigation into a threat made in 2014 to contaminate infant formula with 1080 poison. It was suggested that the investigation could have benefited from examination orders being made against suspected individuals.
- 16.15 Two submitters addressed the issue of whether the Act should allow examination orders to be made against a person suspected of, arrested for, or charged with the offending in question. One supported this, to mirror the powers of SFO,³⁵ while the other submitter did not (but did not provide reasons).

WHY THE EXAMINATION ORDER REGIME SHOULD BE RETAINED

- 16.16 We consider the examination order regime should remain in the Act. We have not identified any compelling reasons for removing it. In addition, any review of the regime should ideally occur *after* it is seen in operation.
- 16.17 We understand that Police is planning to make use of examination orders in the future. The Police 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, many of whom are professionals and business owners/operators. We were told that examination orders are likely to be a valuable investigative tool in that context.
- 16.18 Although examination orders are a coercive tool, there are a number of safeguards and limitations surrounding their use. For example, judicial approval of an examination order is required before Police can subject a person to compulsory examination, and the privilege against self-incrimination is expressly preserved in the Act. In contrast, SFO can exercise its

32 Issues Paper, above n 4, at [10.42].

33 At [10.41]. See, however, our discussion in Chapter 14 at paragraph [14.25]. There, we noted that the wider powers that have been conferred on SFO were introduced in light of international experience at the time (which suggested that traditional investigative powers had been found wanting), and that their existence does not—in and of itself—justify broadening the powers available to other enforcement agencies.

34 Issues Paper, above n 4, at [10.49].

35 The Serious Fraud Office Act 1990 expressly provides that the Director of SFO may examine “any person whose affairs are being investigated” (s 9(1)(a)). There is also case law establishing that the examination power may be used against a person who has been charged: *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).

examination powers simply by issuing a notice to the person to be examined, and the privilege against self-incrimination is removed.³⁶

- 16.19 As for whether the Act should clarify who can be an examinee, on reflection we do not consider that any amendment is necessary. The Act does not appear to prevent an examination order from being made against a person suspected of, arrested for, or charged with the offending in question. However, an examinee can refuse to answer questions where doing so would be likely to incriminate them. If answering questions would be likely to incriminate a person in terms of section 60(1) of the Evidence Act 2006, their non-compliance with the order is justified by the privilege against self-incrimination (which is expressly preserved in section 138 of the Search and Surveillance Act).
- 16.20 We consider that this provides an adequate safeguard. The ability to claim the privilege also makes it unlikely, in practice, that Police would seek an examination order in respect of a suspect/person arrested or charged. Nor is a judge who is considering the application for an examination order likely to be satisfied under section 38 that it is reasonable to subject that person to compulsory examination.³⁷
- 16.21 Finally, we are not convinced that there is any justification for extending the availability of examination orders to a wider range of offences, in the way proposed by a submitter (see paragraph [16.14] above). It would not align with the primary rationale for the regime (to help Police unravel complex financial transactions).³⁸ Furthermore, compulsory examination of a suspect (the example given by the submitter) would be of limited assistance to enforcement agencies given that the privilege against self-incrimination is expressly preserved.

36 And as noted in n 33 above, see our discussion in Chapter 14 at paragraph [14.25].

37 The judge might consider, for example, that compulsory examination of a suspect/person charged or arrested infringes s 23(4) of the New Zealand Bill of Rights Act 1990, which guarantees the right to refrain from making a statement if a person is arrested or detained under any enactment for any offence or suspected offence. As we noted in our Issues Paper, a person required by statute to attend an examination is arguably “detained” for the purposes of that Act (see *Official Assignee v Murphy* [1993] 3 NZLR 62 (HC) and *Police v Smith and Herewini* [1994] 2 NZLR 306 (CA)), so suspects/persons charged with offending could be regarded as “detained ... for [a] suspected offence”: Issues Paper, above n 4, at [10.48].

38 We acknowledge that examination orders are available in a non-business context to help Police investigate both serious and complex fraud and organised crime (which may not involve financial crime). However, this was thought to be necessary because “these types of offending tend to be pervasive, are sometimes difficult to detect, and often involve sophisticated and complex transactions that are not always readily understandable without the assistance of persons involved in those transactions”: Cabinet Business Committee “Law Commission Report Search and Surveillance Powers: Paper 8: Examination Powers” (14 March 2008) CBC (08) 91 at [20]. No one suggested to us that there are particular categories of offending that are so pervasive and difficult to detect that the use of examination orders is needed.



Part 5
OTHER
MATTERS

Chapter 17

Privilege

INTRODUCTION

- 17.1 In our Issues Paper, we described how privileged material in general is protected from disclosure under the Search and Surveillance Act 2012 (the Act). We identified some possible gaps in the process and suggested options for clarifying and strengthening the protective regime.¹
- 17.2 We have dealt with some of the issues we identified in the Issues Paper elsewhere in this Report:
- In Chapter 4, we considered whether the Act should require applications for warrants and orders to identify any privilege issues of which the applicant is reasonably aware. We concluded that they should. To give effect to this, we recommended that the Act be amended to include a principle that powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any individual.
 - In Chapter 12, we considered how the privilege against self-incrimination operates in the context of a request for access information under section 130 of the Act. We recommended clarifying that the privilege only protects a person from having to orally disclose or write down the *content* of access information if that content is itself incriminating.
- 17.3 In this chapter, we discuss the following outstanding issues in relation to the Act's privilege regime:
- whether the ability to claim the privilege against self-incrimination should be removed in the context of production orders;
 - whether production and examination orders should be required to include information about how to claim privilege; and
 - whether the Act sufficiently accommodates the out-of-court resolution of privilege claims.
- 17.4 We conclude that there is no ability for the privilege against self-incrimination to apply to production orders, and recommend the reference to those orders in section 138 be removed. We also recommend that the Act be amended to: require production and examination orders to contain an explanation of relevant privileges and how to claim them; and clarify that out-of-court resolution of privilege claims is possible.

BACKGROUND

- 17.5 The Evidence Act 2006 provides a general regime for claims to privilege in legal proceedings.² Privilege is the ability to withhold certain kinds of oral or written evidence. The person who owns the privilege must claim it to trigger its protective effect. The effect of a successful claim is that the privilege owner can refuse to disclose the evidence in proceedings if they are asked

¹ Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) ch 8 [Issues Paper].

² "Proceeding" is defined in s 4 of the Evidence Act 2006 as a proceeding conducted by a court and any interlocutory or other application to a court connected with that proceeding.

to do so. In some cases, they can also prevent recipients or other persons in possession of the privileged material from disclosing it.³

- 17.6 Some privileges protect the integrity of our adversarial legal system,⁴ such as legal professional privilege,⁵ the privilege against self-incrimination⁶ and the privilege for communications between parties (or between a party and a mediator) when trying to settle a civil dispute or engaging in plea discussions in the criminal context. Other privileges protect relationships that require confidentiality to operate effectively: for example, communications between a person and their minister, a patient and their doctor, or an informant and an enforcement agency.

The protection of privileged material under the Search and Surveillance Act

- 17.7 In its 2007 Report, *Search and Surveillance Powers*, the Law Commission concluded that evidential material for which a claim of privilege would be available in proceedings should also be protected from disclosure during investigations.⁷ To ensure consistency, the Commission recommended adopting the privileges as described in the Evidence Act.

- 17.8 This recommendation is reflected in section 136 of the Search and Surveillance Act, which recognises the following privileges (and one more limited protection from disclosure):⁸

- legal professional privilege, to the extent it forms part of the general law;⁹
- privilege for communications with legal advisers;¹⁰
- privilege for preparatory materials for proceedings;¹¹
- privilege for settlement negotiations, mediation, or plea discussions;¹²
- privilege for communications with ministers of religion;¹³
- privilege in criminal proceedings for information obtained by medical practitioners and registered clinical psychologists;¹⁴
- privilege against self-incrimination;¹⁵
- privilege for informers in relation to identity;¹⁶ and

3 Evidence Act 2006, s 53(3)–(4).

4 In adversarial systems, parties conduct investigations and then present the evidence to an independent fact finder, either a judge sitting alone or a jury. In an inquisitorial system, the judge has an investigative as well as adjudicative role and makes inquiries on their own initiative.

5 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”. It protects confidential communications between a person and their legal adviser from disclosure, to ensure that free and frank advice is given and received; and it also protects some other information that is generated by each party while preparing for litigation from disclosure to the other side.

6 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. For a summary, see Law Commission *The Privilege Against Self-Incrimination* (NZLC PP25, 1996) at [14]–[20].

7 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [12.8]–[12.10].

8 Search and Surveillance Act 2012, s 136. The Evidence Act 2006 also provides judicial discretions (ss 69 and 70) preventing disclosure of confidential material for which privilege cannot be successfully claimed. These are not recognised by the Search and Surveillance Act. There are also discrete privileges in other legislation that are not relevant in this context.

9 Under s 53(5) of the Evidence Act 2006.

10 As described in s 54 of the Evidence Act 2006.

11 As described in s 56.

12 As described in s 57. Section 57 was amended on 8 January 2017 by s 21 of the Evidence Amendment Act 2016 so that the privilege now applies in both civil and criminal proceedings.

13 As described in s 58.

14 As described in s 59.

15 As described in s 60. This privilege allows a person to refuse to provide specific information (oral or written) that would be likely to incriminate them under New Zealand law in relation to an offence punishable by a fine or imprisonment. It applies only to examination and production orders: Search and Surveillance Act 2012, s 138.

16 As described in s 64 of the Evidence Act 2006.

- the limited protection for a journalist in relation to non-disclosure of a source.¹⁷

In this chapter we use the term “privilege” to refer collectively to these privileges and the more limited protection for journalists in relation to their sources.

- 17.9 The Act provides how privilege claims must be managed where powers under the Act are exercised.¹⁸ The Evidence Act determines whether a specific claim to privilege is successful. The Search and Surveillance Act then sets out how privileged material should be dealt with¹⁹ and bars its use in any subsequent proceedings relating to the exercise of the power.²⁰

THE PRIVILEGE AGAINST SELF-INCRIMINATION AND PRODUCTION ORDERS

- 17.10 In our Issues Paper²¹ we explained that section 138 of the Act provides for the privilege against self-incrimination to be claimed in relation to production and examination orders.²² We asked whether there was in fact any scope for that privilege to apply in relation to a production order. That is because the privilege only protects against a person incriminating themselves. It does not protect against disclosure of anything that is incriminating, such as a pre-existing document or other forms of real evidence.²³
- 17.11 Section 60 of the Evidence Act limits the privilege against self-incrimination 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:²⁴
- a statement of fact or opinion 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.
- 17.12 Production orders require the disclosure of documents. Production can be required on an ongoing basis, covering documents not yet in existence.²⁵ However, even where that is the case, the documents are not prepared or created *in response to* a requirement to provide specific information. They must be documents that would be prepared for the normal business purposes of the third party required to produce them.²⁶

17 Under s 68 of the Evidence Act 2006. Section 68 provides protection for a journalist (or their employer) from being compelled to disclose the identity of a source or information enabling that identity to be discovered. The court has discretion to determine that the protection does not apply. To do so, the court must first be satisfied that the public interest in disclosure 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 the facts and opinion to the public by the news media, and the ability of the news media to access sources of fact: Evidence Act 2006, s 68(2).

18 For example, in the search context the Act provides for the right to prevent a search of material for which privilege is claimed, pending the determination of the claim (s 142); it regulates the conduct of searches that extend to lawyers’ premises or material held by lawyers (s 143) or material held by ministers of religion, medical practitioners or clinical psychologists (s 144); and it sets out the interim steps to be taken in relation to the material for which privilege is claimed, pending the resolution of the claim (s 146).

19 For example, it prevents the search of a thing seized or sought to be seized if a privilege claim is upheld: s 142(a).

20 If a privilege claim or the limited protection in relation to journalists’ sources is upheld, 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: s 148.

21 Issues Paper, above n 1, at [8.58]–[8.65].

22 Search and Surveillance Act 2012, s 138.

23 Law Commission *Evidence: Evidence Code and Commentary* (NZLC R55 Vol 2, 1999) at [281]; *Cropp v Judicial Committee* [2008] NZSC 46, [2008] 3 NZLR 774 at [47].

24 Evidence Act 2006, s 51(3).

25 Search and Surveillance Act 2012, s 71(2)(g).

26 See the related discussions in Chapter 14 at paragraphs [14.6]–[14.9].

- 17.13 We therefore questioned (as commentators have done)²⁷ the scope for the privilege to operate in the production order context. We asked whether section 138 should be amended to remove the reference to production orders to avoid confusion.
- 17.14 Submissions from enforcement agencies considered there was no scope for the privilege against self-incrimination to apply in relation to production orders. One other submitter suggested that a forward-looking production order could leave space for “testimonial” documents to be produced, but did not explain how.

Our view

- 17.15 We have been unable to identify any examples of where a forward-looking production order could have testimonial effect. These orders relate to documents that would have been created anyway, regardless of any request by an enforcement officer. Testimonial documents, by definition, are created *in response* to a request from an enforcement officer.
- 17.16 We have therefore concluded that there is no ability for the privilege against self-incrimination to apply to production orders. We recommend that the reference to production orders in section 138 be removed.

PROVIDING INFORMATION ABOUT PRIVILEGE WITH PRODUCTION AND EXAMINATION ORDERS

- 17.17 In our Issues Paper,²⁸ we noted that only search warrants are required by the Act to contain an explanation of the availability of relevant privileges and how they can be claimed.²⁹ There is no corresponding requirement for any other warrant or order.
- 17.18 We acknowledged that in relation to surveillance, the subject will be unaware of the surveillance and therefore unable to claim privilege before any material is seen or heard. However, we could find no rationale for the variation in approach between search warrants, on the one hand, and production and examination orders on the other. We considered that the absence of information about privilege could mean that the recipients or targets of these orders might not know of their ability to make a privilege claim.³⁰ The provisions in the Act for protecting privileged information would then be unable to achieve their intended purpose. We therefore suggested the Act could be amended to require production and examination orders to contain an explanation of the availability of privilege.
- 17.19 There was significant support for this proposal from submitters. No submitters argued against it, although one warned there was potential to create confusion. We took this to refer to the risk of an increase in privilege claims that were either not well-founded or were made as blanket claims.³¹

27 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].

28 Issues Paper, above n 1, at [8.46]–[8.57].

29 Search and Surveillance Act 2012, s 103(4)(i).

30 In Chapter 14 at paragraph [14.111], we recommended that an enforcement officer should take reasonable steps to notify the target of a production order as soon as possible after the order has been executed. The target of a production order is a person who is a suspect in the relevant investigation and whose personal information is the focus of the production order. Notification should include providing the target with a copy of the production order and the associated advice on privilege, to allow for a privilege claim to be made after the fact.

31 The possibility of blanket claims is dealt with in s 147 of the Act, which imposes an obligation on the claimant to particularise the claim to privilege or, if that is not possible, to apply to a judge for directions or relief. The existing advice as to privilege claims that is provided by Police on the search warrant (according to a template that was supplied to us) contains information about that obligation to particularise (in other words, not to make a blanket claim except where particularising it is not possible and the matter must be judicially determined).

Our view

- 17.20 We consider that information about claiming privilege should be provided with production and examination orders, as currently happens with search warrants. That information should:
- explain what privileges are available;
 - explain how privilege may be claimed;³²
 - suggest that a person who may wish to claim privilege can seek legal advice; and
 - clarify that there is no duty on third parties (for example, service providers who hold customer information that is the subject of a production order) to claim privilege on another person's behalf.
- 17.21 Police provided its current excerpt from the search warrant template (which appeared in our Issues Paper as Appendix B).³³ It lists the available privileges and advises a person to seek legal advice if they require further information about the nature or applicability of the privileges. The template also refers to the duty on a claimant to particularise the claim and the ability (under section 146) to apply to the District Court for directions or relief if adequate particularisation is not possible.
- 17.22 That template satisfies all of the requirements set out in paragraph [17.20] above except for the last one. We consider the template should be amended to include that additional information. An adapted version could then be used for production and examination orders. Variations would be required to reflect the different privileges that can apply in those contexts. For examination orders, the information would need to refer to the privilege against self-incrimination. This would not be required for production orders because, as we discussed above, we consider there is no scope for the privilege against self-incrimination to apply.³⁴
- 17.23 Finally, we note the Act does not require that a person who may wish to claim privilege be given the opportunity to seek legal advice *before* a search is carried out (or before a production or examination order is executed). However, as a matter of best practice, we envisage that enforcement officers would give such persons a reasonable opportunity to seek legal advice before executing the search or order. This would be in line with the principle we recommended in Chapter 4, that powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any person. As we explained in Chapter 3, a departure from that principle would run the risk that the search would be found to be unreasonable in terms of section 21 of the New Zealand Bill of Rights Act 1990.

OUT-OF-COURT RESOLUTION OF PRIVILEGE CLAIMS

- 17.24 One submitter (an enforcement agency) identified an issue that was not discussed in our Issues Paper. That is whether the privilege regime in the Act adequately accommodates the resolution of privilege claims without involvement of the court. The submitter noted that the procedures in the Act are predicated on claims being determined in court, as they would be if they were made in proceedings. However, in the investigation context this may not always be necessary. The enforcement agency may accept the privilege claim is valid and reach an agreement with the privilege owner to return the privileged material (if it has already been seized) or to limit the scope of the search to exclude the material. If the search is digital (for

³² That is, by referring to the procedure set out in s 147 of the Search and Surveillance Act 2012.

³³ Issues Paper, above n 1, at 251.

³⁴ See paragraphs [17.10]–[17.16].

example, a search of a computer hard drive), this may involve agreeing on particular search terms or keywords that the agency will use to identify and exclude privileged material.

- 17.25 The Act makes no mention of such consensual arrangements between an agency and the privilege owner. If approached literally, section 142 (the effect of a claim of privilege on search warrants and powers) and section 146 (interim steps pending resolution of that claim) could be interpreted as preventing them.³⁵ For example, although section 146 permits an enforcement officer to secure a thing in respect of which privilege has been claimed, it prohibits them from searching the thing unless the claim is withdrawn or “the search is in accordance with the directions of the court determining the claim of privilege”.³⁶ If a person claims privilege in respect of digital material, for example, this provision may be taken as preventing any further searching of that material without the involvement of the court.

Our view

- 17.26 In our view, it is desirable for the Act to facilitate the out-of-court resolution of privilege claims. This would help to minimise costs for the parties and the courts, and allow issues of privilege to be dealt with in a timely manner. We therefore recommend that the Act should be amended to clarify that claims to privilege do not require resolution by a court if the enforcement agency and the privilege owner agree to exclude certain material from the search and agree on a procedure for isolating that material.
- 17.27 We considered recommending that out-of-court resolution should be conditional upon the privilege owner receiving independent legal advice beforehand. During consultation, some enforcement agencies raised concerns that this would cause delay and queried who would bear the cost of the advice. They also questioned what would happen if a person chose not to obtain legal advice.
- 17.28 We consider it is important that a person claiming privilege has the opportunity to access legal advice. However, we accept that a mandatory requirement would not be practicable. Instead, we consider that as a matter of best practice the person should be informed of their ability to seek legal advice before agreeing to a consensual process for managing a privilege claim and should be given the opportunity to do so.
- 17.29 We recommended above that production and examination orders should be accompanied by information on the available privileges and how to claim them.³⁷ This is already required for search warrants. This information should include a statement to the effect that the recipient of the order may seek legal advice. We consider that if there is any indication that out-of-court resolution of a privilege claim is an option, the enforcement officer should specifically draw the privilege owner’s attention to their ability to seek legal advice.
- 17.30 We note that if an enforcement agency has concerns about a person’s understanding of their situation, it could choose to resolve the privilege claim (and the appropriate ambit of the search) in court under the existing procedures provided by the Act.

35 Section 142 explains the effect of a claim to privilege on search warrants and search powers. The person making the claim of privilege has the right to prevent the search of privileged material and the right to require the return of a copy or access to that material if it is seized or secured by a person exercising a search power, *pending determination of the claim to privilege*. Section 146 describes the interim steps to be taken where the person executing a warrant or exercising a search power is unable to search a thing because a claim of privilege has been made. The person may secure the thing (if the thing is intangible, this can be done by making a forensic copy of the thing) and deliver it to the court *to enable the determination of a claim to privilege by a Judge of that court*.

36 Section 146(c).

37 See paragraphs [17.20]–[17.23].

RECOMMENDATIONS

- R65 The reference to production orders in section 138 (privilege against self-incrimination) should be removed.
- R66 Provisions should be inserted into the Act to require production orders and examination orders to contain an explanation of the availability of relevant privileges and an outline of how those privileges may be claimed.
- R67 A provision should be inserted into the Act to clarify that claims to privilege do not require resolution by a court if the enforcement agency and the privilege owner agree to exclude certain material from the search and agree on a procedure for isolating that material.

Chapter 18

Assistance from intelligence agencies

INTRODUCTION

18.1 Our Issues Paper asked submitters whether the capabilities of the New Zealand Security Intelligence Service (NZSIS) and Government Communications Security Bureau (GCSB) should be available to assist in the performance of police functions, beyond the scope of current police powers. Consideration of this issue was specifically required by our terms of reference (see Appendix 1). In this chapter, we explain why we consider no change to the current law is necessary or justified.

BACKGROUND

18.2 The issue of whether the Search and Surveillance Act 2012 (the Act) should be amended to enable broader use of NZSIS and GCSB's capabilities was raised in the report of the First Independent Review of Intelligence and Security, which was published in February 2016. That review was carried out by Sir Michael Cullen and Dame Patsy Reddy, and considered the legislation that governs the activities of GCSB and NZSIS. In response to the recommendations in that report, Parliament recently enacted the Intelligence and Security Act 2017.

18.3 One of the issues considered in the Cullen/Reddy report was the ability of GCSB and NZSIS to assist other government agencies. At the time, GCSB had an express function under its legislation of assisting New Zealand Police to perform its functions (that is, law enforcement functions),¹ while NZSIS did not. When providing that assistance, GCSB was required to act within the scope of police powers. The report recommended that both GCSB and NZSIS should have this function,² which they now have under the Intelligence and Security Act.³

18.4 The Cullen/Reddy 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*.⁴ The Intelligence and Security Act did not make any changes in this regard. Since this would effectively increase the scope of what Police can do, the report suggested it be considered as part of our review of the Search and Surveillance Act. Accordingly, the issue was included in our terms of reference.

CONSULTATION

Issues Paper

18.5 Our Issues Paper described the functions and powers of GCSB and NZSIS, compared those to the powers of Police under the Act, and explained the (then) existing scope of GCSB

¹ Government Communications Security Bureau Act 2003, s 8C.

² 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) at [5.57] and recommendation 29.

³ Intelligence and Security Act 2017, s 13.

⁴ 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) at [5.59].

and NZSIS's ability to assist law enforcement agencies.⁵ Our analysis suggested there was no significant gap in the ability of GCSB and NZSIS 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 Search and Surveillance Act.⁶ It appeared the main area where there could be scope for increased intelligence agency support for police investigations was at the point of preventing or detecting crime rather than investigating specific offending.⁷

- 18.6 We identified two possible ways in which this issue could, theoretically, be addressed:⁸
- (a) 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
 - (b) 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.
- 18.7 We indicated our preliminary view that neither of these changes was likely to be justified. In relation to option (a), we considered it was 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 would effectively expand police powers through a back door.⁹
- 18.8 As for option (b), we considered this would 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 we noted there could be benefits to such an approach from a community safety perspective, we considered it would fundamentally alter the balance between law enforcement and human rights values in a way that we did not think the New Zealand public would support.¹⁰
- 18.9 We also noted that neither Police nor the intelligence agencies supported such a change. While Police considered that greater assistance from the intelligence agencies might be useful in some cases, the barriers to this occurring were primarily practical rather than legislative.¹¹ We sought submitters' views on this.

Submissions

- 18.10 Almost all submissions that we received on this issue opposed any extension of the ability of GCSB and NZSIS to assist law enforcement. One submitter (the New Zealand Law Society) considered that the current requirement for search and surveillance activity to be carried out where there are reasonable grounds to suspect the commission of an offence and belief that the search or surveillance would obtain evidential material was a "fundamental check" upon intrusive State activities. The Law Society did not consider the case had been made out for any relaxation of that requirement.

5 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [11.9]–[11.35] [Issues Paper]. We also examined the approaches taken in Australia, Canada and the United Kingdom: at [11.36]–[11.38].

6 There was, at the time of writing the Issues Paper, a gap in NZSIS's ability to assist New Zealand Police, but that was remedied by the Intelligence and Security Act 2017.

7 Issues Paper, above n 5, at [11.10]. In other words, GCSB and NZSIS can only assist where the criteria for a warrant or search power under the Search and Surveillance Act 2012 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.

8 At [11.46].

9 At [11.47].

10 At [11.48].

11 At [11.4].

- 18.11 Only one submitter (an enforcement agency) clearly supported such an extension. It did so on the basis that intelligence collected could be used to detect transnational organised crime. However, our understanding is that the (then) existing limitations on intelligence agencies collecting and passing on information relating to transnational crime to enforcement agencies have been addressed under the Intelligence and Security Act.¹²

OUR VIEW

- 18.12 The Intelligence and Security Act 2017 was enacted after we published our Issues Paper. While some aspects of the law changed under that legislation, the functions and powers that we discussed in our Issues Paper remain broadly similar. The most significant change is that GCSB is now able to obtain authorisation to collect intelligence about New Zealanders for certain national security purposes.¹³ This includes collecting intelligence about terrorism and specified serious crimes (such as transnational crimes) where that is necessary to contribute to the protection of national security.¹⁴ As we noted above, NZSIS has also been given an express function of co-operating with and providing advice and assistance to Police – a function that previously only applied to GCSB.¹⁵ These changes should strengthen the ability of NZSIS and GCSB to co-operate with law enforcement agencies, including by collecting intelligence about serious crime and sharing it with the appropriate authorities.¹⁶
- 18.13 Particularly in light of those changes, we remain of the view that any use of intelligence agencies' capabilities for law enforcement purposes beyond the scope of current police powers is unnecessary and would be inappropriate. As we observed in our Issues Paper, while national security has long been recognised as an area where some intrusive monitoring or detection activities are required, strong justification is needed to extend equivalent powers to a law enforcement context. The submissions we received did not convince us that such a justification exists.

12 As we noted in our Issues Paper, GCSB and NZSIS sometimes collect intelligence that has links to crime or law enforcement in the course of performing their intelligence and security functions; and may provide that intelligence to enforcement agencies where it is relevant to preventing or detecting crime punishable by two or more years' imprisonment: Issues Paper, above n 5, at [11.26]–[11.28]. One of the issues the Intelligence and Security Act sought to address was that the definition of "security" in s 2 of the New Zealand Security Intelligence Service Act 1969 was outdated and did not account for collecting intelligence on non-traditional security threats such as cyber threats or transnational crime. Section 58 of the Intelligence and Security Act 2017 now defines the circumstances in which the intelligence and security agencies may take action in pursuit of their national security objective. This includes the identification of serious crime that originates outside New Zealand as well as serious crime involving transnational movement of money, goods or people (s 58(2)(e)).

13 Previously, s 14 of the Government Communications Security Bureau Act 2003 prohibited the interception of New Zealanders' private communications. Under the Intelligence and Security Act 2017, GCSB can collect intelligence about New Zealanders under a "Type 1" intelligence warrant (Intelligence and Security Act 2017, s 53). Type 1 warrants are available in more limited cases than warrants relating to foreign intelligence (Intelligence and Security Act 2017, ss 58–59).

14 Intelligence and Security Act 2017, s 58.

15 Intelligence and Security Act 2017, s 13.

16 The functions of NZSIS and GCSB include sharing intelligence with any person approved by the responsible Minister (Intelligence and Security Act 2017, s 10(b)(iii)) and co-operating with and providing assistance to any public authority (s 10(2)(a)).



Appendices

Appendix 1

Terms of reference

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 2

Glossary

GLOSSARY OF FREQUENTLY USED TERMS	
browser history monitoring	The use of a computer program or device to monitor and/or record the web browsing history of an electronic device or a web user.
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.
covert operations	A broad term that covers operations in which an enforcement officer or another person acting at the direction of an enforcement agency establishes, maintains or uses a relationship with any other person for the covert purpose of obtaining information or providing another person with access to the information by deception (for example, by not disclosing their true motive or identity).
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.
data preservation regime	A regime that requires service providers to preserve data in specific cases for a set period of time where the data at issue is clearly identified in a notice or order and is relevant to a specific criminal investigation or proceeding.
data retention regime	A regime that requires service providers to retain certain types of data for prolonged periods of time (that is, beyond their usefulness for business purposes) in case that data may one day be required for law enforcement purposes.
data surveillance technology	A device, program or other technological aid capable of being used to monitor or record the input of information to, or output of information from, an electronic device.
digital search	A search relating to stored data (as opposed to data in transit).
directed surveillance	The observation or monitoring of an individual's movements or activities in a manner not requiring a surveillance warrant, for example, an enforcement officer following a suspect in a car.
electronic device	Any device that is capable of storing data. This includes computers, mobile phones, tablets, digital cameras, hard drives, USB sticks and memory cards.
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.

GLOSSARY OF FREQUENTLY USED TERMS	
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.
extrasensory technology	Technology that enables the user to observe or detect things that cannot be perceived using natural senses, for example thermal imaging devices, chemical residue detectors or x-ray technology.
Global Positioning System (GPS)	A satellite navigation system used to determine the ground position of an object or person.
International Mobile Subscriber Identity (IMSI)	A number located in a mobile phone's subscriber identification module (SIM) card, which identifies the subscriber.
IMSI catcher / cell-site simulator	A device that mimics a cell tower, forcing mobile electronic devices with SIM cards in the vicinity to transmit data to it. This includes data that can be used to ascertain the location of the device; the identity of the user; and information about the numbers the device has called or sent messages to.
Internet Protocol (IP) address	A unique address that identifies a device on the Internet or a local network.
issuing officer	Defined in section 3 of the Act 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 geographical 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 to and received from. It does not include the content of communications, such as the body of an email.
public surveillance	The monitoring or observation of people, places, things or information that either occurs in public places or relates to information that is publicly available, including "public visual surveillance", "social media monitoring" and "directed surveillance".
public visual surveillance	The use of visual surveillance technology in circumstances not requiring a surveillance warrant. This will be the case where the surveillance occurs in a public place and does not involve: observation and/or recording of private activity in private premises; or observation and/or recording of private activity in the curtilage of private premises for more than three hours in a 24-hour period or eight hours in total.
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.
senior courts	The senior courts are the High Court, Court of Appeal and Supreme Court (Senior Courts Act 2016).

GLOSSARY OF FREQUENTLY USED TERMS

service provider	Private sector businesses that provide a service to customers. This includes telecommunications network operators, internet service providers, banks, electricity and gas suppliers and transport companies.
social media	Internet-based communication platforms that enable users to share information (including messages, videos, pictures and any other content). Examples include Facebook, Twitter, Instagram, Snapchat, web forums and blogs.
social media monitoring	Enforcement officers accessing social media platforms to obtain information about individuals or classes of individuals.
wide area network (WAN)	A computer network that covers a broad geographical area and that may include some local area networks.

Appendix 3

List of submitters and consultees

MAKERS OF SUBMISSIONS OR COMMENTS

- Auckland District Law Society Inc
- Bell Gully
- Chief Judge, District Court of New Zealand
- Chief Justice of New Zealand*
- Crown Law Office*
- Department of Corrections*
- Department of Internal Affairs*
- Electricity Retailers' Association of New Zealand
- Google Inc
- Human Rights Commission*
- Inland Revenue*
- Internet New Zealand*
- Meridian Energy Limited
- Ministry for Primary Industries*
- New Zealand Bankers' Association
- New Zealand Centre for Human Rights, Law, Policy and Practice
- New Zealand Criminal Bar Association
- New Zealand Customs Service*
- New Zealand Law Society
- New Zealand Police*
- New Zealand Police Association
- New Zealand Telecommunications Forum Inc
- Office of the Privacy Commissioner*
- Palmerston North Crown Solicitor
- Royal Federation of New Zealand Justices' Associations Inc
- Spark New Zealand Trading Limited
- Te Hunga Rōia Māori o Aotearoa*
- Trade Me Limited*

- Vodafone New Zealand Limited*
- Warren Young*
- Westpac New Zealand Limited
- Other individual submitters

* indicates where the Law Commission and Ministry of Justice review team also engaged the submitter or commenter during the project (either in person or via teleconference/phone or email).

CONSULTATION LIST

The review team consulted with our Officials Group and Expert Advisory Group (as recognised in the acknowledgements at the beginning of this Report). We also consulted with the following persons and organisations during the course of this review:

- Public Defence Service
- InternetNZ
- Ministry of Transport
- Felix Geiringer

We also sought the views of enforcement agencies and Crown Solicitors with the assistance of the Crown Law Office's Public Prosecutions Unit and the Departmental Prosecutors' Forum.