



INVASION OF PRIVACY: PENALTIES AND REMEDIES

REVIEW OF THE LAW OF PRIVACY
STAGE 3





INVASION OF PRIVACY: PENALTIES AND REMEDIES

REVIEW OF THE LAW OF PRIVACY
STAGE 3

The Law Commission 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:

Right Honourable Sir Geoffrey Palmer SC – *President*

Dr Warren Young – *Deputy President*

Emeritus Professor John Burrows QC

George Tanner QC

Val Sim

The General Manager of the Law Commission is Brigid Corcoran

The office of the Law Commission is at Level 19, HP Tower, 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

National Library of New Zealand Cataloguing-in-Publication Data

Invasion of privacy: penalties and remedies : review of the law of privacy : stage 3.

(Law Commission report ; 113)

ISBN 978-1-877316-84-5 (pbk.)

ISBN 978-1-877316-85-2 (internet)

1. Privacy, Right of—New Zealand. 2. Electronic surveillance—
Law and legislation—New Zealand. I. Title.

II. Series: New Zealand. Law Commission. Report ; no. 113.

342.930858—dc 22

ISSN 0113-2334 (Print)

ISSN 1177-6196 (Online)

This paper may be cited as NZLC R113

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

The Hon Simon Power
Minister Responsible for the Law Commission
Parliament Buildings
WELLINGTON

29 January 2010

Dear Minister

NZLC R113 – INVASION OF PRIVACY: PENALTIES AND REMEDIES

I am pleased to submit to you Law Commission Report 113, *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3*, which we submit under section 16 of the Law Commission Act 1985.

Yours sincerely

A handwritten signature in dark ink, appearing to read 'Geoffrey Palmer', with a horizontal line underneath.

Geoffrey Palmer
President

The Commission's Privacy project has 4 stages. We have already published a study paper *Privacy: Concepts and Issues*, the culmination of stage 1, and a report on *Public Registers*, setting out our findings on stage 2.

The present report completes stage 3. Building on the issues paper we published in 2009, it deals with the remedies and penalties our law provides for invasions of privacy. We do not deal much with the Privacy Act 1993 in this report: that will be the subject of separate study in stage 4 of our project. This report is concerned mainly with the criminal and civil law as it is applied in the courts.

Given the threats to privacy posed by new technology, it is clear to us that the law needs to provide more protection than it currently does. The challenge is to ensure that that protection does not come at the cost of weakening other vital personal and public interests such as freedom of information.

We asked questions in our issues paper about the tort of invasion of privacy confirmed by the Court of Appeal in *Hosking v Runting*. We wanted to know whether such a tort was needed, and if so whether it should be codified in statutory form or left to develop at common law. After full consideration, informed by the submissions on the issues paper, we have decided to recommend that the tort be left to the common law, and indeed that it should be left to the courts to decide whether it should be extended to encompass a tort of intrusion as well.

We found that surveillance is not well regulated by the current law. Technology is developing rapidly and continually creating new ways of invading our privacy. There are legal controls on some kinds of surveillance, but not all. The law is patchy and unsatisfactory, and contains some surprising gaps. We recommend in this report that the law should be rationalised and brought up to date. We recommend that a Surveillance Devices Act should be enacted. This Act would create the criminal offences of trespassing to install a surveillance device; using a device to undertake surveillance of the interior of a dwelling; and using tracking devices. There will be appropriate defences to each. The offences of intimate covert filming and interception of private communications, currently in the Crimes Act 1961, should be transferred to this new Surveillance Devices Act. We also recommend that it should be an offence to publish information obtained in breach of the Act, and that there should be mirror civil liability for breach of its provisions. Private investigators would be bound by the provisions of the new Act like everyone else, and there would no longer be a need for the separate provision regulating surveillance by them alone which currently exists.

In addition, we recommend that the Harassment Act 1997 should be amended to extend its coverage to certain types of surveillance, and that a new offence of voyeurism should be created. We foreshadow that in stage 4 of our review we shall be suggesting that the Privacy Act 1993 needs to be amended to clarify its application to surveillance.

The report also discusses data surveillance. The existing law is capable of handling most types of invasive conduct of this kind, but it is complicated and contains logical anomalies and overlaps. We believe data surveillance merits separate review by a panel of experts.

The use of Closed-Circuit Television (CCTV) surveillance is increasing in both the private and public sectors. It undoubtedly has beneficial uses, but care needs to be taken to ensure that it is used responsibly. The Privacy Commissioner has recently issued CCTV guidelines, and we are content to leave matters there for the time being.

We believe that the reform package we recommend in this report will give citizens protections they do not currently have, and that the balance it achieves between privacy and other interests is right. The recommended new offences are deliberately narrowly defined.

We thank all those who made submissions on the issues paper. We found the submissions most helpful. We also thank the Ministry of Justice and the Office of the Privacy Commissioner for their continuing support and advice.

A handwritten signature in black ink, appearing to read 'Geoffrey Palmer', with a horizontal line underneath.

Geoffrey Palmer
President

ACKNOWLEDGEMENTS We are grateful to the following individuals and organisations who made submissions in relation to this stage of the Law Commission's Review of Privacy:

Accident Compensation Corporation

Auckland District Law Society (Public Issues Committee)

Business New Zealand

Christchurch City Council

Fairfax Media

Fay Roy

Gail Bingham

Investment Savings and Insurance Association

Jane Bruce

Māori Television

Mark Obren

Media Freedom Committee of the Commonwealth Press Union
(New Zealand section)

Ministry of Social Development

Myles Pollard

National Council of Women of New Zealand

Nelson Bays Community Law Centre

New Zealand Institute of Professional Investigators

New Zealand Law Society (Privacy Working Party)

New Zealand Press Council

Nicole Moreham, Senior Lecturer in Law, Victoria University of Wellington

Office of the Privacy Commissioner

Parents' Legal Information Line, Wellington Community Law Centre

RJ Rimmer

Rosemary Tobin, Associate Professor of Law, University of Auckland

Screen Production and Development Association of New Zealand

Selene Mize, Senior Lecturer in Law, University of Otago

Sovereign Limited

Television New Zealand Limited

Ursula Cheer, Associate Professor of Law, University of Canterbury

Whitireia Community Law Centre

Four submissions were received from students in the University of Auckland Media Law Honours Class: Eva Smith, Kieran Hoverd, Alaister Moughan, Rupert Gillies and Tom Price; Tom Pasley, Leigh Walker, Lucas Cooney, Lynn Lai and Jaime Pang; Frances Cummings, Alice Krzanich, Kate Rendall and Elizabeth Whelan; Olivia Upton, Nicola Booth, Bryan Malapaya, Michael O'Brien and Isaac Manase.

We would also like to thank those people who posted comments on our consultation website www.talklaw.co.nz.

In addition, we are grateful to the following individuals and organisations with whom we have met in relation to this stage of our Review, or who have provided comment on drafts of the issues paper and report:

Broadcasting Standards Authority

Ministry of Justice

Office of the Privacy Commissioner

Australian, New South Wales and Victorian Law Reform Commissions

Participants in a consultation meeting with Māori held in June 2008

Participants in consultation meetings with media organisations held in April 2009

Members of the academic reference committee for the Review of Privacy: Ursula Cheer (University of Canterbury); Gehan Gunasekara (University of Auckland); Miriam Lips (Victoria University of Wellington); Selene Mize (University of Otago); Nicole Moreham (Victoria University of Wellington); Steven Price (Victoria University of Wellington); Paul Roth (University of Otago); Rosemary Tobin (University of Auckland)

Judge David Harvey

The Commissioners responsible for this project were John Burrows and Geoffrey Palmer. Legal and policy advisers who worked on this stage of the Review of Privacy were Susan Hall, Joanna Hayward, Sara Jackson and Ewan Morris.





Invasion of privacy: penalties and remedies

CONTENTS

Foreword	iv
Acknowledgements.....	vi
Recommendations	3
Chapter 3	3
Chapter 4	5
Chapter 5	5
Chapter 6	6
Chapter 7	6
Chapter 8	6

CHAPTER 1

Introduction	7
--------------------	---

CHAPTER 2

Reforming the law on surveillance	10
Background.....	10
The existing law on surveillance	12
Law enforcement.....	12
Criminal law	12
Civil law	14
Privacy Act 1993.....	14
Other forms of regulation	15
The case for reform.....	15
The roles of the criminal and civil law	16
Criminal law	17
Civil law	18
Reform of New Zealand surveillance law: an overview	20

CHAPTER 3

A new Surveillance Devices Act.....	22
Primary criminal offences	23
Data surveillance.....	25
Trespass to install a visual surveillance device or interception device.....	28
Visual surveillance	31
Tracking.....	37
Interception	40
Secondary criminal offences.....	51
Disclosure	51
Sale, supply and related matters.....	54
Civil remedies.....	55

CHAPTER 4

The Privacy Act 1993 and surveillance.....56
 The role of the Privacy Act in regulating surveillance56
 Are separate surveillance principles or a surveillance regulator needed?..... 57
 Regulation of specific types of surveillance: CCTV and RFID..... 58
 Improving the Privacy Act’s coverage of surveillance.....63

CHAPTER 5

Other remedies and penalties for intrusion65
 The Harassment Act 1997.....65
 Application to surveillance..... 66
 Voyeurism70

CHAPTER 6

Specific sectors75
 The media.....75
 Regulatory controls..... 77
 Civil and criminal liability: media exemptions and defences 78
 Māori, privacy and the media..... 81
 Private investigators 82
 The workplace.....86

CHAPTER 7

Tort of invasion of privacy.....88
 Do we need the tort at all?.....89
 Should the tort be codified?90
 Partial codification 91
 An intrusion tort?92
 Other civil liability93
 Another tribunal?94

CHAPTER 8

Statutory prohibitions on disclosure.....95
 Are all the existing offences required?96
 Should the inconsistencies within the offence provisions be addressed?97
 Are any new offences required?98

APPENDICES

APPENDIX A

Some further issues relating to interception 102
 Relationship between the offences of interception and computer misuse..... 102
 Are private electronic communications limited to communications between people? 104
 To what extent do the computer misuse offences cover the interception of
 electronic communications? 105
 Reasonable expectation of privacy and different modes of communication..... 106
 Oral communications..... 107
 Electronic communications 108
 Postal mail 109
 Visual surveillance and the interception of communications 110
 Accessing stored communications 110

APPENDIX B

Tort of invasion of privacy: analysis of submissions..... 112



Recommendations

CHAPTER 3

- R1 A Surveillance Devices Act should be enacted providing for criminal offences and a right of civil action in relation to the use of visual surveillance, tracking and interception devices.
- R2 The Surveillance Devices Act should not include “data surveillance devices” as a category of surveillance device, specific data surveillance offences, or the computer misuse offences currently in the Crimes Act.
- R3 The adequacy of existing law to deal with the following should be reviewed: covert surveillance of input of data to or output of data from a computer, and covert access to data stored on a computer. (See also R11.)
- R4 When the computer misuse offences in the Crimes Act are next reviewed, consideration should be given to the issues of civil remedies for computer misuse and whether it should be an offence to disclose information obtained in contravention of the computer misuse offences.
- R5 The Surveillance Devices Act should include an offence of intentionally installing a visual surveillance device or interception device on or within private land, premises or a vehicle, where the installation involves a trespass onto or into the land, premises or vehicle. There should be exceptions to this offence for law enforcement agencies acting in accordance with a warrant or emergency warrantless power and for intelligence organisations acting in accordance with their statutory powers.
- R6 The sections of the Crimes Act dealing with intimate visual recordings should be removed from that Act and included in the new Surveillance Devices Act.
- R7 The Surveillance Devices Act should include an offence of using a visual surveillance device to observe or record the interior of a dwelling with the intention of observing, recording or monitoring the people who reside there, knowing that such observation or recording is done without the consent (express or implied) of the lawful occupiers of the dwelling. In addition to appropriate exceptions for law enforcement and intelligence agencies, the following defences should be available:

- That the accused believed, on reasonable grounds, that at the material time the particular part of the dwelling that was subject to surveillance using a visual surveillance device was being used primarily as a place of work or business.
 - That the accused believed, on reasonable grounds, that the surveillance was necessary:
 - (a) for the protection of the health or safety of any person, or for the protection of public health or safety; or
 - (b) to provide evidence that an offence had been or was being committed or planned;and that the surveillance was no more extensive than reasonably necessary for those purposes.
- R8 The Surveillance Devices Act should include an offence of knowingly installing, using or maintaining a tracking device to determine the geographical location of a person or thing, knowing that the device is installed, used or maintained without the consent of the person, or of the person having lawful possession or control of the thing. In addition to appropriate exceptions for law enforcement and intelligence agencies, it should be a defence to this offence that the use of the tracking device was necessary for the protection of the health, safety or wellbeing of any person, or for the protection of public health or safety, and was no more extensive than reasonably necessary for those purposes.
- R9 The provisions in the Crimes Act providing for interception offences should be removed from that Act and included in the new Surveillance Devices Act.
- R10 The definition of “private communication” for the purposes of the interception offences should be amended to replace the two current criteria with a single “reasonable expectation of privacy” test.
- R11 The review of data surveillance (see R3 above) should include an assessment of the adequacy of the current legal framework for the interception of electronic communications, including the suitability of the reasonable expectation of privacy test for different types of electronic communication, and consideration of the issues discussed in Appendix A.
- R12 Participant monitoring of private communications (both principal party monitoring and authorised outsider monitoring) should be permitted where:
- it is reasonably necessary for the protection of the lawful interests of one or more of the principal parties;
 - there are reasonable grounds to believe that monitoring is in the public interest; or
 - the participant monitoring is conducted by a law enforcement officer acting in the course of duty.
- R13 Further consideration should be given to whether participant monitoring should be a permitted exception to the interception of non-oral electronic communications.
- R14 The Surveillance Devices Act should make it an offence for a person to disclose information (including images and recordings) if that person knows, or ought reasonably to know, that the information was obtained directly or indirectly by the use of a surveillance device in contravention of the criminal provisions of the Act.

- R15 It should continue to be an offence for a provider of internet or other communication services to disclose information obtained by intercepting private communications when undertaking maintenance of a communication service.
- R16 The Surveillance Devices Act should provide that it is an offence to make, sell or supply a surveillance device, or software that can convert a device into a surveillance device, knowing that the device or software is to be used to undertake surveillance in contravention of the criminal provisions of the Surveillance Devices Act; or to promote or hold out a device or software as being useful for the carrying out of surveillance in contravention of the Act.
- R17 The Surveillance Devices Act should provide for a right of civil action by any person affected by a breach of any of the criminal provisions. Standard tort remedies should be available, and the defences should be the same as for the relevant offence.

CHAPTER 4

- R18 The Privacy Act should provide that one of the functions of the Privacy Commissioner is to report regularly to Parliament on developments in surveillance and surveillance technologies, and their implications for New Zealand.
- R19 Both Closed-Circuit Television (CCTV) and Radio-Frequency Identification (RFID) should be regulated within the Privacy Act framework, rather than under specific statutes or regulations. The Privacy Commissioner should continue to monitor the adequacy of existing law to deal with these technologies. If a more specific regulatory framework is considered necessary in future, the option of developing codes of practice under the Privacy Act should be considered.
- R20 A code of ethics for private security personnel who install, advise on, operate and monitor CCTV systems should be made under the Private Investigators and Private Security Guards Act 1974 or any replacement statute. The code of ethics should address legal and ethical requirements in relation to privacy. Any prescribed training in relation to CCTV for private security personnel should also cover privacy obligations.

CHAPTER 5

- R21 Section 4 of the Harassment Act 1997 should be amended by adding a new paragraph (ea): “Keeping that person under surveillance”.
- R22 Section 3 of the Harassment Act 1997 should be amended by providing that a pattern of behaviour can be constituted either by a single protracted act or by doing a specified act on at least two separate occasions within a period of 12 months.
- R23 It should be an offence to deliberately observe without consent, whether with or without a device, for purposes of sexual gratification, conduct of the kind defined in the Crimes Act 1961, section 216G(1)(a).
- R24 Section 30 of the Summary Offences Act 1981 should be repealed and replaced with a provision that makes it an offence to look repeatedly or for a prolonged period into a dwellinghouse for the purpose of obtaining sexual gratification. The offence should not be limited to night time.

-
- CHAPTER 6
- R25 Section 52 of the Private Investigators and Security Guards Act 1974 should be repealed and the corresponding clause of the Private Security Personnel and Private Investigators Bill should be deleted. However, these changes should only be made after the following recommendations have been implemented:
- the enactment of a Surveillance Devices Act, as recommended in chapter 3;
 - the amendment of the Harassment Act 1997, as recommended in chapter 5; and
 - the introduction of a code of ethics for private investigators, as recommended in R26 below.
- R26 A code of ethics or code of conduct for private investigators should be made under the Private Investigators and Security Guards Act, or under the Private Security Personnel and Private Investigators Bill if that Bill is enacted. The code should address issues of privacy and the use of surveillance by private investigators.
- R27 Additional offences involving serious invasions of privacy should be added to the lists of disqualifying offences for private investigators and their employees in the Private Investigators and Security Guards Act or the Private Security Personnel and Private Investigators Bill. These offences should include the existing intimate covert filming offences, and the new surveillance device offences that we recommend in this report.
-
- CHAPTER 7
- R28 The tort of invasion of privacy recognised in *Hosking v Runting* should be left to develop at common law.
- R29 Any recognition and development of a tort of intrusion into solitude, seclusion and private affairs should be left to the common law.
-
- CHAPTER 8
- R30 When next each of the statutes imposing a criminal penalty for disclosing information is reviewed, the question should be addressed of whether the offence provision is necessary or whether the Privacy Act 1993 provides adequate protection.
- R31 Whenever one of the statutes which imposes a penalty for disclosure of information is reviewed, attention should be paid to its consistency with analogous provisions.

Chapter 1

Introduction

- 1.1 This report sets out the Law Commission’s recommendations with regard to stage 3 of our Review of Privacy (“the Review”). According to our terms of reference for the Review, in stage 3 the Commission is to consider and report on:
 - (a) the adequacy of New Zealand’s civil remedies for invasions of privacy, including tortious and equitable remedies; and
 - (b) the adequacy of New Zealand’s criminal law to deal with invasions of privacy.
- 1.2 Stage 3 should be seen in the context of the Commission’s wider Review, which consists of four stages. Stage 1 was a high-level policy overview, assessing privacy values, changes in technology, international trends and other matters, and their implications for New Zealand law. At the conclusion of stage 1, the Commission produced a study paper, *Privacy: Concepts and Issues*, which provides background information for the later stages of the Review.¹ Stage 2 considered the law relating to public registers to see whether it requires alteration as a result of privacy considerations or emerging technology. Stage 2 has also been completed with the publication of a final report.² Implementation of the recommendations of that report is on hold pending completion of stage 4 of the Review, which involves a comprehensive review of the Privacy Act 1993 with a view to updating the Act. The Commission will be producing an issues paper for stage 4 of the Review early in 2010, and calling for public submissions on the issues raised in that paper. Although the Privacy Act is not the focus of this stage 3 report, it is impossible to ignore the Act in any consideration of privacy law in New Zealand, and in chapter 4 of this report we give particular consideration to the role of the Privacy Act in regulating surveillance.
- 1.3 We released an issues paper for stage 3 of the Review in March 2009 and called for public submissions. We received 35 submissions from individuals and organisations. We also set up a website on which people could make comments about some of the issues raised in the issues paper, and we received a number

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

2 New Zealand Law Commission *Public Registers: Review of the Law of Privacy: Stage 2* (NZLC R101, Wellington, 2008).

of thoughtful comments on these issues via the website. The submissions we received have influenced our recommendations in this report, particularly on issues about which there was consensus or near-consensus among submitters.

- 1.4 The issues paper analysed the existing law dealing with invasions of privacy in New Zealand and in certain overseas jurisdictions. The paper then considered issues and options for reform of the law, focusing on two areas. First, we looked at disclosure of private facts, and in particular at the tort of invasion of privacy by publicity given to private facts. The Court of Appeal found in the case of *Hosking v Runting*³ that such a tort exists in the common law of New Zealand. Secondly, we examined intrusions into solitude and seclusion and prying into people's private affairs. In particular, we looked in some detail at how the law deals with surveillance.
- 1.5 This report focuses on our recommendations for law reform in relation to the two areas just mentioned. It does not repeat the analysis of the existing law that can be found in the issues paper.
- 1.6 Surveillance has emerged in the course of our Review as the area in which the gaps and inconsistencies in the law are particularly significant, and it is the focus of the bulk of this report. For reasons set out in chapter 2, we believe the law dealing with surveillance in New Zealand is in need of reform. We should emphasise that we are not talking here about the authorised use of targeted surveillance by law enforcement and regulatory agencies. Law enforcement surveillance was the subject of recommendations in an earlier Law Commission report, *Search and Surveillance Powers*, and the Commission's recommendations in that report are to be implemented by the Search and Surveillance Bill currently before Parliament.⁴ What we are examining in this report is the general criminal and civil law dealing with surveillance.
- 1.7 Chapter 3 sets out our most important recommendation for reform of surveillance law, the creation of a new Surveillance Devices Act. This Act would provide for both criminal offences and a right of civil action in relation to use of visual surveillance, interception and tracking devices. It would include some existing offences from the Crimes Act and some new offences. It would close some gaps in the existing law, and complement protections provided by the Privacy Act 1993. We discuss the role of the Privacy Act in regulating surveillance in chapter 4, and identify some ways in which the Privacy Act's coverage of surveillance could be improved. We will consider reforms to the Privacy Act in relation to its coverage of surveillance further in stage 4 of our Review. Chapter 5 discusses some other areas in which the law could better protect against surveillance and other intrusions. We recommend some changes to the Harassment Act 1997 to ensure that it clearly applies to harassing surveillance. We also recommend some reforms that would criminalise voyeurism in a more comprehensive manner than at present. Chapter 6 deals with surveillance in three particular sectors or contexts: the media, private investigators, and the workplace. Our main recommendations in chapter 6 are for the repeal of specific legal restrictions on surveillance by private investigators, providing the Surveillance

3 [2005] 1 NZLR 1.

4 New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007); Search and Surveillance Bill 2009, no 45-1.

Devices Act and the amendments to the Harassment Act 1997 discussed in chapters 3 and 5 are enacted and a new code of ethics for private investigators is introduced.

- 1.8 Chapter 7 discusses the tort of invasion of privacy, including both the existing *Hosking* tort and the possibility of a tort of intrusion into seclusion and private affairs. In the issues paper we asked whether the common law tort should be retained and, if so, whether it should be put on a statutory basis. Based largely on the submissions we received, we have decided that both the *Hosking* and the intrusion torts should be left to develop at common law. Chapter 8 then considers whether existing statutory prohibitions on disclosure of personal information need to be reformed in any way, including by repealing existing offences, adding new offences, or addressing inconsistencies between different offences. We make some recommendations for further review of these provisions in future.

Chapter 2

Reforming the law on surveillance

- 2.1 This chapter provides some background in relation to surveillance and how it is currently dealt with in the law, drawing on information from the issues paper for this stage of our Review. We then make the case for reforming the law in relation to surveillance, and briefly outline the recommendations for reform that will be discussed in more detail in later chapters.

BACKGROUND

- 2.2 In our issues paper, we provided some background information in relation to surveillance, which we summarise briefly here.⁵ We defined surveillance, for the purposes of our discussion, as “the use of devices intentionally to monitor, observe or record people’s actions or communications”.⁶ Surveillance can include:⁷
- watching and visual recording, using devices such as binoculars or cameras;
 - listening and intercepting, including using devices to record or listen to conversations, or to intercept emails, text messages, or other electronic data;
 - locating and tracking by such means as Global Positioning System (GPS) devices and cellphone location data; and
 - monitoring data by methods such as computer hacking, spyware, and keystroke logging.
- 2.3 The technologies of surveillance are developing apace. Surveillance devices are becoming smaller, cheaper, less noticeable, and easier to use. Information obtained through surveillance is being digitised, allowing it to be combined with digital data from other sources, analysed in new ways, and disseminated widely (especially over the internet). Technological convergence means that devices can increasingly be used for multiple purposes, or can form part of a larger surveillance network. For all of these reasons, surveillance is becoming more pervasive in everyday life.⁸

5 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington, 2009) ch 8 [Privacy Stage 3 issues paper].

6 *Ibid*, 181.

7 *Ibid*, 188-189.

8 *Ibid*, 190-191; see also New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, Wellington, 2008) 136-139.

2.4 Surveillance is used in a wide range of contexts, including:⁹

- state security and intelligence;
- law enforcement and regulation (including at the local government level);
- environmental and road traffic regulation;
- personal and public safety and security;
- commercial;
- domestic;
- research;
- media;
- workplace; and
- private investigation.

As a number of submitters on our issues paper emphasised, many of these uses are beneficial to individuals and society. In particular, they can help to deter and detect crime or serious wrongdoing, and can provide information that helps us to understand what is going on in our immediate environment or in the wider society.

2.5 At the same time, it is important to recognise that surveillance can have significant negative effects, particularly:¹⁰

- use of information obtained through surveillance for criminal purposes such as identity theft, blackmail, fraud or burglary;
- a chilling effect on the exercise of civil liberties;
- loss of anonymity;
- stress and emotional harm;
- the creation of a record of personal information which can be stored permanently, disseminated widely, analysed in great detail, and taken out of context;
- excessive collection of personal information;
- insecurity and loss of trust;
- use for voyeuristic or other questionable purposes;
- discrimination and misidentification; and
- desensitisation to surveillance, leading to a narrowing of people's reasonable expectations of privacy.

2.6 Information about public attitudes to surveillance is limited, but suggests that attitudes vary depending on the type of surveillance under consideration, and to some extent on factors such as gender and ethnicity. For example, there is a relatively high level of concern about monitoring of internet use and email, whether by internet providers wanting to deliver targeted

9 Privacy Stage 3 issues paper, above n 5, 192-200, and ch 12 for media, workplace, and private investigators.

10 Ibid, 201-204.

advertising or by employers seeking to identify inappropriate computer use. Concern about closed-circuit television (CCTV) surveillance, by contrast, is low, and indeed there seems to be a high level of support for CCTV based on a perception that it helps to make communities safer.¹¹

THE EXISTING LAW ON SURVEILLANCE

- 2.7 Our issues paper looked at the current law dealing with privacy generally, and with surveillance in particular, and set out a number of hypothetical scenarios which illustrate the coverage of the existing law.¹² Readers should go to the issues paper for further details of the law summarised below.

Law enforcement

- 2.8 As noted in chapter 1, this report does not deal with the use of targeted surveillance as part of law enforcement operations. The Law Commission has already reported on law enforcement surveillance, and the Search and Surveillance Bill currently before Parliament is based on the recommendations of our *Search and Surveillance Powers* report.¹³ If enacted, the Bill will replace existing provisions in other legislation governing surveillance by law enforcement agencies.
- 2.9 In addition, section 21 of the New Zealand Bill of Rights Act 1990 provides for the right to be secure against unreasonable search and seizure. The courts have treated some forms of surveillance conducted by law enforcement agencies as searches for the purposes of section 21, although the Court of Appeal has not yet ruled definitively on the matter.¹⁴

Criminal law

Crimes Act 1961

- 2.10 Part 9A of the Crimes Act 1961 is entitled “Crimes against personal privacy”, and deals with interception and intimate covert filming. The interception provisions create offences of intercepting a private communication by means of an interception device, disclosing private communications that were unlawfully intercepted, and selling or supplying interception devices.¹⁵ The provisions relating to intimate covert filming deal with situations in which a visual recording is made, without the knowledge or consent of the subject, of:
- a person who is in a place which would reasonably be expected to provide privacy, when that person is naked or nearly naked, engaged in sexual activity, or engaged in showering, toileting or other activity that involves dressing or undressing; or
 - a person’s naked or undergarment-clad private parts, if the recording is made from beneath or under a person’s clothing or through a person’s outer clothing where it is unreasonable to do so.¹⁶

11 Ibid, 204-206.

12 Ibid, chs 2, 3 and 9; the scenarios are at 224-234.

13 New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007) ch 11 [*Search and Surveillance Powers* NZLC R97]; Search and Surveillance Bill 2009, no 45-1, cls 42-67.

14 *Search and Surveillance Powers* NZLC R97, 318-319.

15 Crimes Act 1961, ss 216B-216D.

16 Ibid, s 216G.

It is an offence to make, possess in certain circumstances, publish, import, export or sell such intimate visual recordings.¹⁷

- 2.11 The Crimes Act also includes provisions relating to crimes involving computers, and these provide some protection against surveillance in the form of covert access to personal data through methods such as computer hacking and use of spyware. The computer crimes sections of the Act create offences of accessing a computer for a dishonest purpose; damaging or interfering with a computer system; selling, supplying or possessing software for committing computer crime; and accessing a computer without authorisation.¹⁸

Summary Offences Act 1981

- 2.12 The Summary Offences Act 1981 does not deal directly with surveillance, but does include some offences that may be able to be used against surveillance in certain circumstances, particularly in the case of voyeuristic visual surveillance. Section 4(1)(a) creates an offence of behaving in an offensive or disorderly manner in or within view of any public place. In two cases involving the same man, prosecutions were brought for offensive behaviour in a public place after a man surreptitiously photographed young women near a school and in a library. In both cases the man was convicted in the District Court; in one case his conviction was upheld on appeal in the High Court and the Court of Appeal, but in the other the High Court overturned his conviction.¹⁹ Both cases illustrated the difficulty of applying section 4(1)(a) of the Summary Offences Act to covert photography. Another offence that has some relevance to visual surveillance is “peeping or peering” into a dwellinghouse at night,²⁰ which we discuss further in chapter 5. Although peeping and peering cases usually involve a person looking directly, without the aid of a device, through a window, it is possible that it could apply to a situation in which a visual surveillance device is used. Section 29 of the Summary Offences Act may also sometimes be called in aid: it involves being found on enclosed premises without reasonable excuse.

Other offences

- 2.13 Section 52 of the Private Investigators and Security Guards Act 1974 makes it an offence for a person, in the course of business as a private investigator, to take or cause to be taken, or use or accept for use, a photograph, film or video recording of another person without that other person’s consent. It also makes it an offence to record or cause to be recorded another person’s voice or speech without consent. We discuss this provision further in chapter 6.
- 2.14 It is conceivable that surveillance could form part of a pattern of behaviour constituting the offences of intimidation or criminal harassment,²¹ but only in conjunction with other, more threatening actions.

17 Ibid, ss 216H-216J.

18 Ibid, ss 249-252.

19 *R v Rowe* [2005] 2 NZLR 833 (CA); *Rowe v Police* (12 December 2005) HC DN CRI 2005-412-000051 John Hansen J.

20 Summary Offences Act 1981, s 30.

21 Ibid, s 21; Harassment Act 1997, s 8.

Civil law

- 2.15 As we note in chapter 7, the Court of Appeal in *Hosking v Runting* left open the question of whether an intrusion tort exists in New Zealand law. An intrusion tort could deal directly with the invasion of privacy involved in the act of surveillance itself, as opposed to the disclosure of information obtained through surveillance. We also refer in chapter 7 to the tort of breach of statutory duty. This may provide a civil remedy in relation to some existing statutes that protect privacy, even though the statute in question does not expressly create such a remedy. The tort of breach of statutory duty is, however, beset by uncertainty, and we will be recommending that a new statute criminalising certain types of surveillance should expressly provide for a civil remedy as well.
- 2.16 Other areas of law that may provide civil remedies for surveillance include:
- trespass, where the installation of surveillance devices involves unauthorised access to land or objects;
 - nuisance, if the surveillance unreasonably interferes with a person's right to use or enjoyment of his or her land (for example, in the case of camera surveillance into a person's home by a neighbour);
 - breach of confidence, but only in relation to the disclosure of confidential information obtained through surveillance; and
 - harassment, if the surveillance fits within one of the "specified acts" listed in section 4 of the Harassment Act 1997 (the existence of a wider harassment tort in New Zealand law is uncertain).

Each of these options for obtaining civil remedies will apply to surveillance only in certain circumstances, and there is a significant degree of uncertainty about the extent to which they cover surveillance.

Privacy Act 1993

- 2.17 The Privacy Act 1993 regulates the way in which personal information is collected, held, used and disclosed. Agencies that deal with personal information must comply with twelve privacy principles that are set out in the Act, and if they fail to do so a complaint can be made to the Privacy Commissioner. Surveillance usually results in the collection of personal information, and information collection is one of the main purposes for which surveillance is used.²² A question has been raised about whether the current wording of the Act limits its coverage of surveillance as far as the privacy principles relating to collection of information are concerned.²³ However, the Privacy Commissioner considers that the collection principles do apply to surveillance, and in any case information obtained through surveillance is clearly covered by the remaining principles. While all of the privacy principles may be relevant to surveillance, principle 4 is of particular note as it can be used to address the intrusive nature of the surveillance itself, rather than dealing only with the information obtained

22 It is also used to influence behaviour, and to seek pleasure or gratification (voyeuristic surveillance): Privacy Stage 3 issues paper, above n 5, 183-184.

23 Ibid, 56-57. The privacy principles dealing with collection of information are information privacy principles 1 to 4: Privacy Act 1993, s 6.

through surveillance. Principle 4 states that personal information shall not be collected by means that are unlawful or unfair, or that intrude unreasonably upon the personal affairs of the individual concerned.

Other forms of regulation

2.18 The Privacy Act does not apply to the news media in relation to their news activities.²⁴ Privacy in the broadcast and print media is regulated by the Broadcasting Standards Authority (a statutory body that enforces broadcasting standards pursuant to the Broadcasting Act 1989) and the Press Council (a voluntary body established by the print media industry) respectively. Both bodies have principles and standards that can be used as the basis for complaints about surveillance activities by the media, such as the use of hidden cameras or microphones.²⁵ We discuss regulation of media surveillance further in chapter 6.

2.19 In addition, there are a number of other relevant policies and voluntary standards:²⁶

- guidance and policies on the use of CCTV from the Office of the Privacy Commissioner, the New Zealand Police, and local councils;
- the voluntary RFID Consumer Protection Code of Practice, which deals with commercial use of Radio Frequency Identification technology; and
- the codes of practice of the New Zealand Marketing Association and the Market Research Association of New Zealand, which deal, among other things, with the use of recording devices by marketers and market researchers.

THE CASE FOR REFORM

2.20 The Law Commission has reached the conclusion that there is a need for reform of New Zealand law relating to surveillance. As we have previously mentioned, we are talking here about the law governing society as a whole, rather than the specific law governing the use of surveillance by law enforcement and intelligence agencies. There are a number of reasons why we believe reform is warranted.

2.21 First, a legal framework is required within which the benefits of surveillance for individuals and for society can be balanced against the need for protection against invasions of privacy and other negative effects of surveillance. Such a framework needs to include some boundaries beyond which certain types of surveillance activities are clearly unacceptable. It also needs to include flexible principles for dealing with the much larger body of surveillance activities that may be acceptable in some circumstances but not in others, or that are acceptable providing that both the surveillance itself, and the handling of information obtained by means of it, comply with certain standards.

2.22 Secondly, the legal framework to which we have just referred exists already in part in New Zealand, but is not sufficiently comprehensive. The criminal law includes some notable gaps: in particular, there are no offences for the use of tracking devices, and only very specific offences relating to visual surveillance. The civil law is uncertain in its application to surveillance, and applies only in

24 Privacy Act 1993, s 2(1), definition of “agency”.

25 Privacy Stage 3 issues paper, above n 5, 64-69, 286-287.

26 Ibid, 222-223.

particular circumstances. The Privacy Act provides important principles for controlling surveillance and regulating the handling of information obtained through surveillance, but there are a number of ways in which its coverage could be improved. Some laws, such as those relating to the broadcast media and to private investigators, apply only to particular sectors.

- 2.23 Thirdly, the introduction of the Search and Surveillance Bill raises the need for counterpart provisions dealing with criminal and civil liability for surveillance outside the context of law enforcement activity. The issue of criminal and civil liability of private persons engaging in surveillance was not considered as part of the Commission's *Search and Surveillance Powers* report; instead, the Commission recommended that this issue should be considered separately as part of a wider review of privacy protection in New Zealand.²⁷ The introduction of the Search and Surveillance Bill highlights certain anomalies, such as the fact that law enforcement officers will require a warrant to use a tracking device yet it is not an offence for the general public to use such devices (although the installation of the device could involve trespass to goods or an offence such as conversion of a vehicle).
- 2.24 Fourthly, New Zealand's laws for dealing with surveillance are in danger of falling behind those of other comparable countries, especially Australia. Three Australian states and one territory now have comprehensive Surveillance Devices Acts.²⁸ These Acts create criminal offences for the use of surveillance devices, and also deal with surveillance by law enforcement agencies. The Australian Law Reform Commission and the New South Wales Law Reform Commission have recommended the creation of a statutory cause of action for invasion of privacy that would create civil liability for, among other things, invasion of privacy by unauthorised surveillance.²⁹ The Victorian Law Reform Commission (VLRC) is currently inquiring into the law relating to surveillance in public places,³⁰ and it is likely that it will report within a similar timeframe to our own. While we may not reach the same conclusions as the VLRC on all issues, the running of the two reviews in parallel creates a significant opportunity for New Zealand and Victoria to learn from each other as our reform proposals are developed and discussed.
- 2.25 For all of the above reasons, we think that there is a need for reform of New Zealand's laws dealing with surveillance, and that the time is right to embark on such reform. This will involve some major changes and some more limited modification of existing laws. We provide an overview of our proposed reforms at the end of this chapter.

THE ROLES OF
THE CRIMINAL
AND CIVIL LAW

- 2.26 The Surveillance Devices Act that we propose in chapter 3 will provide for criminal offences involving the use of surveillance devices, with matching civil remedies for breaches of the criminal provisions. Both the criminal and the

27 *Search and Surveillance Powers* NZLC R97, above n 13, 327, 422-423.

28 Surveillance Devices Act 1998 (WA); Surveillance Devices Act 1999 (Vic); Surveillance Devices Act 2007 (NSW); Surveillance Devices Act 2007 (NT). See also Workplace Surveillance Act 2005 (NSW).

29 Australian Law Reform Commission *For Your Information: Review of Australian Privacy Law* (ALRC R108, Sydney, 2008) ch 74; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC R120, Sydney, 2009).

30 Victorian Law Reform Commission *Surveillance in Public Places* (VLRC CP7, Melbourne, 2009).

civil law involve enforcement by the courts. There is also an important role for regulatory frameworks that provide remedies outside the courts. The Privacy Act is one such regulatory framework, and we consider its role in controlling surveillance in chapter 4.

- 2.27 We discussed the roles of the criminal and civil law, and principles for when each should be used, in our issues paper.³¹ In general, criminal penalties serve to mark society's disapproval of an offence, vindicate societal interests by punishing offenders, and deter potential future offenders. Civil remedies compensate individuals for the harm they have suffered, or prevent the harm from occurring or continuing by mechanisms such as injunctions or restraining orders. There are also practical considerations: the standard of proof is lower in civil proceedings; law enforcement powers of investigation and arrest are available in criminal cases; criminal proceedings can be brought by the Police where there is no one willing or able to bring civil proceedings; and the costs of criminal proceedings are borne by the state rather than the individual.
- 2.28 As we observed in our issues paper, it will sometimes be appropriate for the same conduct to attract both criminal and civil penalties and remedies. We believe that surveillance is one area in which this is the case.

Criminal law

- 2.29 There is a social need for conduct to be criminalised if the conduct causes significant harm to individuals or to the collective interests of the wider society, and if the general public would consider the conduct to be sufficiently serious to warrant criminal penalties. We have discussed the general harms of surveillance briefly above, and we discuss in chapter 3 the specific harms addressed by our proposed offences. Any offences must be carefully targeted to meet the social need, and should not be drawn so broadly as to potentially catch conduct which the public would not consider deserving of punishment.
- 2.30 The criminal law has a role in establishing norms by making it clear that certain conduct is unacceptable. The very fact that particular conduct is an offence will be enough to prevent law-abiding citizens from engaging in such conduct. In the case of surveillance, the criminal law lets responsible members of professions such as journalism and private investigation know that particular types of surveillance are socially unacceptable. Information about the limits established by the criminal law can be provided in training materials and codes of ethics for such professions. The criminal law also plays a role in setting limits for the use of surveillance by law enforcement officers. Such officers are subject to the criminal law just as much as anyone else, unless they are operating under warrant or some specific exemption from the general criminal law.
- 2.31 There will always be some people who are willing to breach social norms, and for such people the threat of punishment by the criminal law may be effective in deterring them from engaging in particular conduct. This may be particularly true for surveillance, which generally requires some planning. A person contemplating undertaking surveillance is likely to have time to

31 Privacy Stage 3 issues paper, above n 5, 121-123; see also Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (2001 edition, most recently amended 2007) 251-255.

consider the consequences of such action, including the possibility of facing criminal sanctions. The norm-setting and deterrent roles of the criminal law will only be effective, however, if the conduct that is prohibited is defined with sufficient precision to allow members of the public to know in advance whether or not particular actions will be criminal.

- 2.32 Because of the role of the criminal law in establishing norms and deterring proscribed conduct, making particular conduct an offence may go a long way towards ensuring that such conduct does not occur very often. Thus, the fact that there are few prosecutions for particular offences does not necessarily mean that the offences are ineffective. It is a different matter, however, if prosecutions are not brought because an offence is seen as too trivial to justify investigation and enforcement by the Police. Making conduct a criminal offence has the advantage that the conduct becomes subject to investigation and prosecution by the state, rather than affected individuals having to rely on their own resources to take legal action.
- 2.33 The investigative powers of the Police can be particularly helpful in detecting and providing evidence of covert surveillance. As the Commission noted in relation to intimate covert filming, in many cases the subjects of surveillance will be unaware that someone has been secretly monitoring or recording them, or that images or other records obtained through such surveillance have been distributed. Furthermore, “[w]hen subjects do become aware [that they have been under surveillance] they are likely to want the intrusion stopped immediately.” If they have sufficient evidence, Police are able to take immediate action by arresting a person engaging in illegal surveillance.³²
- 2.34 We believe that certain forms of surveillance are sufficiently objectionable that they should be subject to criminal sanctions. We see a legitimate role for the criminal law in prohibiting particular types of surveillance (subject to specific defences and exceptions), with a view to clearly establishing that such conduct is unacceptable and deterring those who might otherwise engage in it. We further believe that those forms of surveillance that are clearly unacceptable should be subject to investigation and prosecution by the state. In considering the scope of the offences, we are very conscious of the need to define the prohibited conduct as precisely as possible and to limit the offences to only the most objectionable forms of surveillance.

Civil law

- 2.35 Criminalising the most objectionable types of surveillance can help to prevent such surveillance from occurring and can allow the state to investigate and punish it when it does occur. In general, however, the criminal law does not directly address the harm suffered by those who have been subject to surveillance; that is the role of the civil law. We believe that, where conduct has occurred that would constitute a criminal offence under the new Surveillance Devices Act, the victims of such conduct should have a right of civil action in the courts to seek remedies such as damages or injunctions. As the Commission said in *Intimate Covert Filming*: “Civil remedies can be specifically tailored to redress

32 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) 25 [*Intimate Covert Filming* NZLC SP15].

the particular harm to the individual, and the processes and outcomes for the individual can be more personally restorative and meaningful than the ordeal of a criminal trial.”³³

- 2.36 The Commission previously recommended that complaints under the Privacy Act were the most appropriate means by which to provide a civil remedy for intimate covert filming, and we recommended some amendments to the Privacy Act in order to facilitate this.³⁴ A number of those who made submissions on our issues paper likewise argued that the Privacy Act already provides an adequate and appropriate civil remedy for surveillance.
- 2.37 We continue to believe that the Privacy Act is an important and effective tool for regulating surveillance. In many cases, a complaint to the Privacy Commissioner will also be the most appropriate way of providing a remedy for surveillance (including surveillance that would not constitute an offence under the proposed Surveillance Devices Act). Bringing a civil action in court is an expensive and daunting prospect, and the Privacy Act complaints process is more accessible for most people. In chapter 4 we discuss some ways in which the Privacy Act’s coverage of surveillance could be improved and clarified. As part of our review of the Privacy Act in stage 4 of this Review, we will be proposing some amendments to the Act to clarify its application to surveillance. Even if the Privacy Act were to be amended in the ways we propose, however, we still believe a civil remedy should be available in the courts, for a number of reasons.
- 2.38 First, the Privacy Act is focused on informational privacy, and complaints under the Act must be based on breach of one of the *information* privacy principles. It will not always be the best vehicle, therefore, for dealing with surveillance complaints that may be as much or more about intrusions into spatial privacy. Secondly, the Act does not (with one very specific exception) create legal rights that are enforceable in the courts.³⁵ Any complaint under the Act must first go through the Privacy Commissioner’s investigation and mediation process, which may result in an agreed settlement but does not result in a binding ruling. Only if this process does not produce a satisfactory resolution can the complainant proceed to the Human Rights Review Tribunal, which can grant remedies such as damages or orders restraining the defendant from continuing or repeating the surveillance. Even then, the Tribunal does not have available to it the full range of remedies that can be obtained in the courts: only the courts can grant injunctions, for example, and the courts can award heavier damages than the Tribunal is able to award. Recourse to the courts is, therefore, a more direct route by which to obtain a decision, and may lead to more satisfactory remedies in some cases. Thirdly, the Privacy Act contains some significant exclusions and exceptions. One important exclusion is that the Act does not apply to the news media in relation to their news activities.³⁶ Our recommendations for surveillance

33 Ibid, 26.

34 Ibid, 35-37.

35 Privacy Act 1993, s 11.

36 Ibid, s 2(1), definition of “agency”.

offences are not directed at the media, but there may be cases in which members of the news media commit these offences. In such cases, a civil remedy should be available.

- 2.39 The existence of another option for obtaining civil remedies for some forms of surveillance will not undermine the Privacy Act, in our view. On the contrary, the enactment of a Surveillance Devices Act would strengthen the Privacy Act by making certain types of surveillance unlawful. Principle 4 of the Privacy Act provides that personal information shall not be collected “by unlawful means”. Any collection of information by means of surveillance of a kind that would be an offence under the Surveillance Devices Act will be unlawful, and there will be a strong basis for a complaint of a breach of principle 4 in relation to such surveillance. In addition, both the Law Commission and the Privacy Commissioner have recommended that section 56 of the Privacy Act, which provides for an exception to the Act in relation to personal information collected or held by an individual for the purposes of his or her personal, family or household affairs, should be amended so that it does not apply to personal information collected unlawfully.³⁷ We will be proposing as part of our review of the Privacy Act that section 56 should be amended in this way. If both the Surveillance Devices Act and the amendment to section 56 of the Privacy Act are enacted, the “personal affairs” exception will no longer apply to information obtained by unlawful surveillance. This will allow Privacy Act complaints to be made in some cases which were previously prevented from succeeding by section 56.
- 2.40 We believe there is a strong case for the Surveillance Devices Act to provide for a civil remedy in the courts, to sit alongside the Act’s criminal sanctions and the remedies available under the Privacy Act. This will give victims of unlawful surveillance a right of direct access to the courts to seek damages or other suitable remedies for the harms they have suffered. As we discuss in chapter 7, a right of civil action for breach of statutory duty could be found to exist by the courts in any case, but we think it is preferable to provide expressly for it.

REFORM OF
NEW ZEALAND
SURVEILLANCE
LAW: AN
OVERVIEW

- 2.41 The most significant reform we recommend is the enactment of a new Surveillance Devices Act dealing with civil and criminal liability for surveillance. The Act would:
- create criminal offences for certain uses of visual surveillance, interception and tracking devices;
 - include the existing intimate covert filming and interception offences from the Crimes Act (although with some modifications to the current provisions); and
 - provide that the criminal offences are also enforceable by civil actions brought by victims of the offences.

We discuss this recommendation further in chapter 3.

³⁷ *Intimate Covert Filming* NZLC SP15, above n 32, 37; Privacy Commissioner *Third Supplement to First Periodic Review of the Operation of the Privacy Act* (report by the Privacy Commissioner to the Minister of Justice, December 2003) 6-7.

2.42 We see the Privacy Act and the Privacy Commissioner as having very important roles to play in regulating surveillance. Some amendments are needed to the Act to clarify its application to surveillance. We also recommend that some surveillance issues, such as regulation of CCTV, are best handled by guidance from the Privacy Commissioner or by a code of practice made under the Privacy Act. In addition, we believe the Privacy Commissioner is well placed to undertake ongoing review of developments in surveillance and their implications for New Zealand, and to make recommendations for further reform when appropriate. The role of the Privacy Act in regulating surveillance is discussed further in chapter 4.

2.43 Our other key recommendations in relation to surveillance are that:

- the Harassment Act 1997 should be amended so that it applies more clearly to harassing surveillance;
- certain gaps in the law with respect to voyeuristic observation, whether with or without a device, should be closed; and
- section 52 of the Private Investigators and Security Guards Act 1974 should be repealed, but only after the enactment of the new Surveillance Devices Act, the amendments to the Harassment Act, and the creation of an enforceable code of ethics for private investigators.

These recommendations are discussed in chapters 5 and 6.

Chapter 3

A new Surveillance Devices Act

- 3.1 We recommend in this chapter the enactment of a Surveillance Devices Act that will provide for criminal offences involving:
- the installation of visual surveillance or interception devices where this involves trespass on private property or private vehicles;
 - intimate covert filming (the existing offences from the Crimes Act);
 - visual surveillance, using a device, of the interior of a private dwelling;
 - use of a tracking device to determine the location of a person or thing;
 - interception of private communications (the existing offences from the Crimes Act, with some modifications);
 - disclosure of information obtained through unlawful surveillance; and
 - sale, supply and promotion of surveillance devices for unlawful purposes.

We also recommend that the Act should provide for a right of civil action in the courts for people affected by breaches of the criminal provisions.

- 3.2 We noted in the last chapter that criminalisation is not to be resorted to lightly. But in this case there are sound reasons for recommending criminal offences. First, surveillance technology is developing at great speed, and its potential is virtually limitless. It is important to put boundaries in place to control its harmful use before it is too late. Secondly, it is already criminal to engage in certain types of surveillance: interception by listening device and computer, and intimate covert filming, in particular. It is anomalous to have no provision about tracking, and very little about visual surveillance. The current law has not kept up with the times. Our recommendations fill gaps in that law so as to make it consistent and bring it up to date. Thirdly, we recommend later in this report that private investigators be in no different position from other citizens: the current restraints on them are unreasonable. Yet there have to be general provisions which control how far they and other professions such as paparazzi photographers, and indeed anyone, can go. Fourthly, four of the Australian states and territories have moved in the direction of criminalising the types of surveillance with which we are here concerned. They all do it in slightly different ways, but in all cases the message is the same: that it is important to make a demonstration that there need to be strong sanctions to control the most objectionable types of intrusion. Our recommendations will bring us into line with those states.

- 3.3 In what follows, we have been careful to confine our recommendations for the creation of offences narrowly, and to catch only the most objectionable forms of conduct. Other forms of intrusion which are not covered may still be redressable by the civil law, under the Harassment Act 1997, and under the jurisdiction of the Privacy Commissioner.
- 3.4 We thus believe the enactment of a Surveillance Devices Act will fill some significant gaps in New Zealand law; consolidate all of the provisions relating to unlawful surveillance in one Act; make clear that there is a right of civil action for breaches of the criminal provisions; complement the Search and Surveillance Bill; and bring New Zealand law more closely into line with surveillance legislation in a number of Australian states and territories.

RECOMMENDATION

- R1 A Surveillance Devices Act should be enacted providing for criminal offences and a right of civil action in relation to the use of visual surveillance, tracking and interception devices.

PRIMARY CRIMINAL OFFENCES

- 3.5 In this section we set out our recommendations for the primary offences of carrying out certain forms of surveillance. Our recommendations for related offences, such as disclosure of information obtained through surveillance, appear in a later section of this chapter. Before discussing the detail of the offences, we need to explain some decisions we have made about the overall scope of the criminal provisions of the Act.
- 3.6 First, we recommend that the Act should be limited to surveillance conducted using devices. As we discussed in our issues paper, there are a number of features of surveillance by the use of devices that distinguish it from observation using the unaided senses, and make it of particular concern. Surveillance devices enhance the ordinary senses and thereby allow people to see, hear and monitor others in ways that would not be possible otherwise; allow people to observe and monitor others without the knowledge of those who are the subjects of surveillance; and allow the actions and communications of others to be recorded.³⁸ Recording, in turn, creates a permanent record of an event or communication, which can then be analysed closely, combined with other information, and disseminated widely. Recording also creates the danger that information can be used and interpreted in ways that are removed from the original context and therefore misleading.³⁹ There are, in addition, pragmatic reasons for recommending that the Act should be limited to surveillance using devices: it makes it easier to identify clear boundaries for the offences, and it is easier to prove that surveillance has taken place if a device is involved.⁴⁰

³⁸ New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington, 2009) 181-182 [Privacy Stage 3 issues paper].

³⁹ *Ibid.*, 202.

⁴⁰ *Ibid.*, 181.

- 3.7 Secondly, we recommend that the offences should be specific rather than generic. A generic approach would not distinguish between different types of surveillance device. Instead, the terms “surveillance” and “surveillance device” could be defined by statute, and surveillance by means of any surveillance device could be prohibited in certain circumstances (most likely when it is conducted covertly). A specific approach, by contrast, creates offences relating to particular categories of surveillance device, such as visual surveillance devices or interception devices.⁴¹ We indicated in our issues paper that we preferred the specific approach, and this is the approach that we now recommend. The specific approach is consistent with existing surveillance offences in New Zealand (interception and intimate covert filming), with the Surveillance Devices Acts in Australia, and with the Search and Surveillance Bill. As we have indicated above, the criminal law needs to be as precise as possible, and to target conduct that is particularly serious in its consequences. We believe it would be difficult, if not impossible, to make offences precise and targeted under a generic approach. A specific approach provides clearer parameters and greater certainty about the conduct that would constitute an offence. We note, however, that the specific approach runs the risk of being overtaken by developments in technology that may lead to the creation of surveillance devices that do not fit within the categories specified in the Act. It is therefore important to periodically review whether changes in technology give rise to a need to amend the law. In chapter 4 we recommend that the Privacy Commissioner should keep developments in surveillance technology under review.
- 3.8 Thirdly, we recommend that the Act should deal with three categories of surveillance device: visual surveillance devices, interception devices and tracking devices. These are the three types of surveillance device covered by the surveillance provisions in the Search and Surveillance Bill. They are also broadly consistent with the categories in Surveillance Devices Acts in Australia.⁴² We think they adequately cover the field of surveillance devices currently in use.
- 3.9 Fourthly, the criminal offences and civil actions we recommend should not be inconsistent with the Search and Surveillance Bill currently before Parliament. That Bill deals with surveillance by law enforcement agencies, and prescribes when they must obtain warrants to engage in certain surveillance activities. In all cases an officer lawfully acting under warrant, or other statutory authorisation, is excluded from the offences we recommend. In some cases the conduct constituting an offence is narrower than the activity for which a warrant is required. Thus, in relation to visual surveillance, whereas a warrant is to be necessary for a law enforcement officer to undertake surveillance of private activity in any private premises, our recommended offence provisions are confined to surveillance of the interior of a dwelling. Likewise, whereas under the Bill a warrant will be required to undertake prolonged surveillance of the curtilage of private premises, we do not recommend that any surveillance of the curtilage of a dwelling be an offence. This is not to say that such surveillance without a warrant will not fall foul of the civil law, the Harassment Act or the

41 *Ibid*, 241-243.

42 The Australian statutes at the state and territory level deal with “listening devices” rather than the broader category of “interception devices”, but interception of communications passing over a telecommunications system is covered by the Telecommunications (Interception and Access) Act 1979 (Cth). Some Australian Acts also include a category of “data surveillance devices”.

Privacy Act: it is just that we have not gone to the length of recommending that it be an offence. The non-correspondence of the two sets of provisions is not an inconsistency. Likewise, law enforcement officers validly acting under a warrant or other statutory authorisation would not be liable to civil action under the Surveillance Devices Act. The civil actions we recommend mirror the offences. These immunities from criminal and civil liability for law enforcement officers are reinforced by clauses 158 to 161 of the Search and Surveillance Bill.

Data surveillance

3.10 In contrast to some Australian surveillance device statutes, we do not recommend the inclusion in the Surveillance Devices Act of “data surveillance devices” as a category of surveillance device, or of specific offences relating to data surveillance.⁴³ “Data surveillance device” is defined in the Surveillance Devices Act 2007 (NSW) as meaning “any device or program capable of being used to record or monitor the input of information into or output of information from a computer, but does not include an optical surveillance device”.⁴⁴ It appears to us that specific data surveillance offences are not needed in New Zealand, because they will already be covered in one of three ways:

- If a private electronic communication, such as an email, is intercepted by means of an interception device while the communication is taking place or is in transit, an interception offence will be committed.⁴⁵
- If spyware is installed on a computer without authorisation, this is likely to constitute the offence of damaging or interfering with a computer system, and could also involve accessing a computer without authorisation.⁴⁶
- If a person gains access to data on a computer by “hacking” into the computer, this will be a computer misuse offence: either accessing a computer system for a dishonest purpose or accessing a computer system without authorisation.⁴⁷

3.11 However, while we do not recommend the creation of new data surveillance offences, we have not looked in detail at the adequacy of existing laws to deal with covert surveillance of the input of data to or output of data from a computer, or covert access to data stored on a computer. In our issues paper, we asked a question about the adequacy of the existing computer misuse offences to deal with matters such as the use of spyware, and about whether a review of these offences is required. There was little evidence of dissatisfaction with the current law in the submissions we received, and only a few submissions supported a review of the law. Nonetheless, we think the adequacy of existing law (including, but not limited to, the computer misuse and interception offences)

43 Surveillance Devices Act 2007 (NSW), s 10; Surveillance Devices Act 1999 (Vic), s 9; Surveillance Devices Act 2007 (NT), s 14. The data surveillance device offences in the Victorian and Northern Territory statutes apply only to law enforcement officers.

44 Surveillance Devices Act 2007 (NSW), s 4(1). There are similar definitions in the Victorian and Northern Territory Surveillance Devices Acts.

45 Crimes Act 1961, ss 216A, 216B.

46 Ibid, ss 250, 252; see discussion in Privacy Stage 3 issues paper, above n 38, 213, 233-234.

47 Crimes Act 1961, ss 249, 252.

to deal with covert data surveillance should be reviewed.⁴⁸ Although the computer crimes were enacted and the interception offences amended relatively recently (in 2003), technology is developing rapidly. We therefore recommend that the review should take place within the next few years, and should involve experts in computing and computer security. We believe it is not necessary to wait for the review of data surveillance to take place before enacting the proposed Surveillance Devices Act. This is because there are already protections in place for data surveillance, while the Act which we recommend addresses areas where the current law does not provide adequate protection. Nor have we been made aware that the current law on data surveillance is causing serious practical problems.

- 3.12 The review of data surveillance should include consideration of whether interception of non-verbal electronic communications should be treated differently from interception of oral communications, an issue which we raise in the section on interception below. It should also consider the issue, which was discussed in our issues paper, of “skimming” of data from Radio-Frequency Identification (RFID) chips.⁴⁹ If the existing legal framework is found to be adequate, the review could consider other strategies for dealing with spyware and related problems. Such strategies could include technical measures and public education.⁵⁰
- 3.13 We considered the option of including the existing computer misuse offences, which are currently in the Crimes Act,⁵¹ in the new Surveillance Devices Act. As we have just indicated, these offences help to provide protection against covert data surveillance. Despite this, we do not think that they would fit naturally into the new Act. There are differing views on the extent to which anti-hacking laws are primarily intended to protect against invasion of privacy and loss of control over information, as opposed to protecting the integrity of computer systems.⁵² Clearly, however, they are not directed solely at dealing with data surveillance, and this is even more true of the offence of damaging or interfering with a computer system. The computer misuse offences are currently located within the part of the Crimes Act dealing with crimes against rights of property, rather than crimes against personal privacy. Moreover, these offences do not necessarily involve the use of a device that is separate from the computer in question: they can be committed by direct access to a computer terminal. They would therefore sit awkwardly within a statute based on use of surveillance devices. We recommend that they should stay within the Crimes Act.

48 The Australian Government conducted such a review, focusing on spyware, in 2004-2005: Australian Government *Outcome of the Review of the Legislative Framework on Spyware* (Department of Communications, Information Technology and the Arts, 2005); Australian Government *Spyware Discussion Paper* (Department of Communications, Information Technology and the Arts, 2005) [Australian Government *Spyware Discussion Paper*].

49 Privacy Stage 3 issues paper, above n 38, 254.

50 See Australian Government *Spyware Discussion Paper*, above n 48; Australian Government *Taking Care of Spyware* (Department of Communications, Information Technology and the Arts, 2005).

51 Crimes Act 1961, ss 248-254.

52 Neil MacEwan “The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future” [2008] Crim LR 955, 956-957. The Law Commission said that computer misuse offences should protect both information and systems: New Zealand Law Commission *Computer Misuse* (NZLC R54, Wellington, 1999) 13-14.

- 3.14 One consequence of this is that the civil remedy which we recommend should form part of the Surveillance Devices Act will not be available in relation to computer crimes. The Law Commission considered in our Electronic Commerce project the possibility of creating a statutory tort that would provide a right of action against a person who had breached criminal legislation dealing with computer misuse, and had thereby caused loss or obtained a benefit.⁵³ We did not recommend the creation of such a tort at that time, but did not rule it out as an option for the future.⁵⁴ The Law and Order Committee, when reporting on the Bill that introduced the computer misuse offences, rejected a suggestion that civil remedies for computer misuse should be included in the Bill.⁵⁵ We recommend that the question of a civil remedy for computer misuse should be revisited whenever the computer misuse offences come under review. The civil remedy issue could form part of the review of data surveillance that we are recommending.
- 3.15 We also note that at present the computer crimes provisions of the Crimes Act do not make it an offence to disclose information that was obtained by committing a computer misuse offence. This seems anomalous, given that there are offences for disclosing information obtained in breach of the interception and intimate covert filming provisions of the Crimes Act. Later in this chapter we recommend that the Surveillance Devices Act should make it an offence to disclose information obtained in contravention of the criminal provisions of the Act. We believe there should be a similar provision in relation to computer misuse offences in the Crimes Act, and recommend that the inclusion of a disclosure offence should be considered when the computer misuse offences are next reviewed.
- 3.16 Finally, while we do not recommend the inclusion of data surveillance offences in the Surveillance Devices Act at present, we note that one outcome of the review of the adequacy of existing law to deal with covert data surveillance could be an amendment to the Act to include data surveillance offences at some time in the future.

RECOMMENDATION

- R2 The Surveillance Devices Act should not include “data surveillance devices” as a category of surveillance device, specific data surveillance offences, or the computer misuse offences currently in the Crimes Act.

RECOMMENDATION

- R3 The adequacy of existing law to deal with the following should be reviewed: covert surveillance of input of data to or output of data from a computer, and covert access to data stored on a computer. (See also R11.)

53 New Zealand Law Commission *Electronic Commerce: Part Two: A Basic Legal Framework* (NZLC R58, Wellington, 1999) 98-101.

54 New Zealand Law Commission *Electronic Commerce: Part Three: Remaining Issues* (NZLC R68, Wellington, 2000) 34-35.

55 Law and Order Committee “Crimes Amendment Bill (No 6) and Supplementary Order Paper No 85” (2001) 19.

RECOMMENDATION

- R4 When the computer misuse offences in the Crimes Act are next reviewed, consideration should be given to the issues of civil remedies for computer misuse and whether it should be an offence to disclose information obtained in contravention of the computer misuse offences.

Trespass to install a visual surveillance device or interception device

- 3.17 We recommend the creation of a new offence of *intentionally installing a visual surveillance device or interception device on or within private land, premises or a vehicle, where the installation involves a trespass onto or into the land, premises or vehicle.*
- 3.18 Some of the worst cases of surveillance involve trespassing in order to install visual surveillance or interception devices. Consider the following scenarios:
- A secretly installs an audio recorder, connected to the telephone system, in the house of B, his ex-partner. The recorder activates automatically when the receiver of the phone is lifted, and records B's telephone conversations.⁵⁶
 - C installs hidden cameras in the bedroom of his ex-partner, D, and uses them to film D.⁵⁷
 - E, a journalist, installs a hidden audio recording device in the car of F, a celebrity. E can activate the device in order to record F's conversations.
 - G covertly installs a camera in the board room of Company X, in order to obtain intelligence about Company X's activities for the benefit of one of its competitors.
- 3.19 Two things are particularly objectionable about scenarios such as these. First, trespass is in itself an intrusion into privacy and an interference with property rights. It is a violation of people's right to control access to their private property and to preserve a space in which they can legitimately be free from unwanted intrusions. Secondly, installing a surveillance device allows surveillance and invasion of privacy to continue long after the trespass is over. Both of these features, we believe, would give rise to strong feelings of violation and hurt on the part of a person who discovers that he or she has been subject to surveillance by means of a visual surveillance or interception device installed on private property.
- 3.20 There are a number of existing criminal provisions relating to trespass to land and vehicles, but most have some shortcomings in terms of their ability to deal with trespass to install a surveillance device:
- Criminal trespass under the Trespass Act 1980 applies only after a person has been warned to leave or stay off a property.⁵⁸ It is therefore not suited to dealing with trespass that takes place without the knowledge of the occupier

56 Based on the facts of *R v Stephens* (14 July 1997) CA 156/97 Blanchard J.

57 Based on the alleged facts of *Police v Wright* (28 October 2008) DC AK CRI-2008-004-004596 Judge Aitken. Note however that in this case the defendant was not convicted of a charge of intimate covert filming.

58 Trespass Act 1980, ss 3, 4.

of the property, as will generally be the case with trespass done in order to install a covert surveillance device.

- There are also offences of being found on property without reasonable excuse, being found loitering at night on land on which a dwelling house is situated, and trespass on a ship.⁵⁹ These offences suffer similar defects with regard to the covert installation of surveillance devices to the offences under the Trespass Act: the person must be found on the property or, in the case of trespass on a ship, must have been warned to leave the ship.
- In some cases, entering a property, without authority, to install a surveillance device could constitute burglary, but only if the entry is to a building (which includes an enclosed yard) or ship and is done with the intent of committing a crime.⁶⁰ Installing a surveillance device is not itself a crime, so this offence would only apply if it could be shown that the entry and the installation of the surveillance device were for the purpose of committing another offence, such as intercepting a private communication or making an intimate visual recording.
- Entering or interfering with a vehicle in order to install a surveillance device could constitute the offence of conversion of a vehicle.⁶¹

3.21 These existing provisions provide only partial coverage for situations in which a person goes onto property without authority in order to install a surveillance device. Furthermore, we think there is a strong case for having a specific offence that deals with trespass for the purpose of installing a surveillance device, in order to clearly indicate that this is unacceptable and to provide penalties that are appropriate to the seriousness of the offence. There is also a civil remedy available in the tort of trespass, but we think the type of trespass covered by our proposed new offence is sufficiently serious that it should be criminalised.

3.22 There are two main elements to the proposed new offence. First, there must be entry to property without the consent of the lawful occupier, or the person having lawful control or possession in the case of a vehicle. In other words, there must be a trespass. The offence could be committed regardless of whether or not the person is actually found on the property, and regardless of whether or not the person has been warned off the property. Trespass is not a narrow concept. It is also committed when a person who has a licence to enter property for a limited purpose uses the entry for another purpose to which the occupier would not have consented had he or she known of it.⁶² Thus, the offence we are recommending would be committed when a person gains entry to a property under false pretences: for example, by pretending to be a tradesperson who is there to install or fix something other than a surveillance device. Likewise, the offence would be committed by a person who is admitted by the occupier for a legitimate purpose, but who also has a second, undisclosed, purpose of installing a device: the real plumber, for example, who is called by the occupier to fix a

59 Summary Offences Act 1981, ss 29, 30(1)(b), 31.

60 Crimes Act 1961, s 231.

61 Ibid, s 226(2).

62 *TV3 Network Services Ltd v Fahey* [1999] 2 NZLR 129, 135; *TV3 Network Services Ltd v Broadcasting Standards Authority* [1995] 2 NZLR 720, 732.

water cylinder, but who is also secretly employed by a private investigator to bug the premises. It would be desirable to define “trespass” in the legislation to clearly capture cases like this.

- 3.23 Secondly, there must be installation of a visual surveillance device or interception device by means of such entry. The offence is committed even if there is no evidence that the surveillance device has in fact been used to carry out visual surveillance or interception. On the other hand, if there is trespass and use of a surveillance device but no installation, this offence is not committed, although another may be.⁶³ So, for example, the offence would not be committed if a person entered a house when the occupants were not there and filmed inside the house, or if someone gained admission to a property and recorded there using a camera or microphone concealed on his or her person. While such actions may well constitute significant invasions of privacy, and may be covered by another offence or civil remedy, we think the trespass-based offence should only cover installation of a device. This is because installation allows the surveillance, and therefore the harm, to continue after the person leaves the property. In addition, where a hidden camera or microphone is carried by someone who gains entry by deception, the subject of the surveillance is at least aware of the other person’s presence and is able to modify his or her behaviour accordingly.
- 3.24 We do not think there should be any defences relating to the public interest or to protection of private interests. There are times when it is legitimate to install a visual surveillance or interception device on private property in order to investigate crime or serious wrongdoing. However, the intrusion on privacy constituted by installing such devices is such that it should only occur with the consent of the lawful occupier or in accordance with a warrant or an emergency warrantless power.
- 3.25 The fact that a surveillance device can be installed on private property with the consent of the lawful occupier, or the possessor or controller of a vehicle, means that the offence will not apply to various situations, such as:
- installation of security cameras in a home or business to protect people or property;
 - installation of hidden cameras by an employer in a workplace to detect theft by an employee; or
 - installation of cameras in a property by a television company, with the consent of the occupier, as part of a “hidden camera” trial of tradespeople for a consumer affairs programme.

We think it is appropriate that situations such as these should be excluded from the criminal offence, and we note that such situations will still be covered by other laws such as the Privacy Act, the Broadcasting Act, or employment law. People are entitled to install surveillance devices on property they own or occupy, or to agree to the installation of such devices, even if the devices are used to film

63 Depending on the circumstances, another surveillance device offence may be committed: visual surveillance of the interior of a dwelling (a proposed new offence discussed below), or interception of a private communication.

others covertly. Consideration may need to be given to how “occupier” should be defined, and to how the offence should apply to property with multiple occupiers.⁶⁴

- 3.26 We recommend that this offence should not apply to the installation of tracking devices. The scope of the tracking device offence which we recommend below is such that, where a tracking device is installed on a vehicle, it must be without the consent of the person having lawful possession or control of the vehicle for the offence to be committed. Thus, there is no need for the offence discussed in this section to apply to tracking devices.

RECOMMENDATION

- R5 The Surveillance Devices Act should include an offence of intentionally installing a visual surveillance device or interception device on or within private land, premises or a vehicle, where the installation involves a trespass onto or into the land, premises or vehicle. There should be exceptions to this offence for law enforcement agencies acting in accordance with a warrant or emergency warrantless power and for intelligence organisations acting in accordance with their statutory powers.

Visual surveillance

- 3.27 We did not receive a great deal of comment in submissions about reforms to the criminal law relating to visual surveillance. Our recommendations are, however, broadly consistent with the submission of the New Zealand Law Society, which supported a new visual surveillance device offence in principle, but said that any new visual surveillance offences should be tightly circumscribed and limited to cases of trespass. We have recommended a new trespass-based offence above, and in this section we recommend another new offence which, while not based on trespass, is limited to private dwellings.
- 3.28 Visual surveillance devices for the purposes of the Surveillance Devices Act should mean devices capable of being used to watch or record visually, apart from devices such as spectacles used to correct subnormal vision to normal levels. Visual surveillance devices include binoculars, telescopes, and cameras capable of recording still or moving images (including cameras that are part of multi-function devices such as cellphones).
- 3.29 At present, the only visual surveillance device offences are those relating to intimate covert filming. We recommend that the intimate covert filming offences should be included in the Surveillance Devices Act, along with a new offence of visual surveillance of a private dwelling.

⁶⁴ The question of consent in the case of private premises with multiple occupants is discussed in Law Reform Commission of Hong Kong *Privacy: The Regulation of Covert Surveillance: Report* (Hong Kong, 2006) 12-14 [*The Regulation of Covert Surveillance* LRC Hong Kong].

Visual surveillance in public places

- 3.30 We discussed the criminal law’s treatment of visual surveillance in public places in our issues paper, and asked whether the criminal law dealing with intrusive visual surveillance in public should be reformed in any way.⁶⁵ There was little support in submissions for any extension of the criminal law’s coverage of visual surveillance in public places. Currently, the types of intimate covert filming known as “up-skirting” and “down-blousing” are criminal offences regardless of where they take place,⁶⁶ as is visual recording by a private investigator without consent.⁶⁷ In some circumstances, visual surveillance may constitute offensive behaviour in a public place.⁶⁸
- 3.31 With the exception of “up-skirting” and “down-blousing”, we think visual surveillance in public will very rarely, if ever, be so offensive that it should be a criminal offence. We do not think it is possible to frame a new criminal offence for these rare instances without running the risk of catching conduct that should not be criminalised, including filming and photography by the media. While not well-suited to dealing with covert surveillance,⁶⁹ the offence of offensive behaviour in a public place may sometimes be capable of being used to prosecute particularly offensive visual surveillance. The Privacy Act and the Harassment Act will also provide remedies for visual surveillance in public that breaches the privacy principles or constitutes harassment. We do not, therefore, recommend any change to the existing criminal law as it applies to visual surveillance in public places.

Intimate covert filming

- 3.32 The provisions in the Crimes Act dealing with intimate visual recordings⁷⁰ should be removed from that Act and placed in the Surveillance Devices Act. We do not recommend any substantive changes to those provisions. We noted in our issues paper a possible ambiguity about the wording of the “up-skirting” offence,⁷¹ and the relevant wording could be amended to address this when the provision is included in the new Act.

RECOMMENDATION

- R6 The sections of the Crimes Act dealing with intimate visual recordings should be removed from that Act and included in the new Surveillance Devices Act.

65 Privacy Stage 3 issues paper, above n 38, 208-209, 245-246.

66 Crimes Act 1961, ss 216G(1)(b), 216H.

67 Private Investigators and Security Guards Act 1974, s 52. See further discussion of restrictions on surveillance by private investigators in chapter 6.

68 Summary Offences Act 1981, s 4(1)(a).

69 Privacy Stage 3 issues paper, above n 38, 245.

70 Crimes Act 1961, ss 216G-216N.

71 Privacy Stage 3 issues paper, above n 38, 246, discussing the wording of s 216G(1)(b).

Visual surveillance of a private dwelling

3.33 We recommend the creation of a new offence of *using a visual surveillance device to observe or record the interior of a dwelling with the intention of observing, recording or monitoring the people who reside there, knowing that such observation or recording is done without the consent (express or implied) of the lawful occupiers of the dwelling*. As we discuss below, the term “dwelling” is intended to be wider than “dwelling house” or “home”.

3.34 The following scenarios illustrate the kinds of situations that would be covered by this offence:

- The marriage of a prominent political figure is rumoured to be ending. Using a long-lens camera, a newspaper photographer takes pictures of him and his wife eating a meal together in their house, and the photographs are published.⁷²
- A well-known actor is recovering in hospital from a serious head injury. Newspaper journalists enter his room without permission and photograph him while he is in a confused state. The photographs are published.⁷³
- A private investigator, seeking evidence for use in a Family Court case, enters the home of H while she is not there and films the interior of the house.⁷⁴
- The same private investigator is admitted to H’s house under a false pretence and uses a camera concealed on his person to film H’s interactions with her children.

The offence would cover a person standing outside the dwelling and using a visual surveillance device to look into the interior; a person installing a visual surveillance device within the dwelling and using it to observe or record the interior; and a person carrying a camera into the dwelling and using it to record the interior.

3.35 This offence protects the right of people to be free from observation that goes beyond what can be seen with the naked eye, and to be free from visual recording, in their homes and other places where they reside and have a reasonable expectation of privacy. The law has long recognised the special place of the home as a private space and a place of refuge from the outside world, and the home is specifically linked to the right to privacy in international human rights instruments.⁷⁵ The right of people to be left alone and to be free from unwanted

72 Based loosely on an incident discussed on “Media 7”, TVNZ 7, 16 July 2009. In that incident, the photograph was of a couple eating a meal on the balcony of their home, rather than inside the house, and the newspaper did not publish the photograph.

73 Based on the facts of *Kaye v Robertson* [1991] FSR 62.

74 Based on conduct described in Hank Schouten “007 Spy Sting in Marital Bust-up” (24 May 2005) *Dominion Post* Wellington 1; “Bogus Spy Operation Costs Employee \$70k” *CresseyLaw.co.nz Newsletter* (July 2005).

75 Universal Declaration of Human Rights, art 12, and International Covenant on Civil and Political Rights, art 17, both state that people should be protected from interference with “privacy, family, home or correspondence”. Justice Eady discussed the importance of privacy in the home in *McKennitt v Ash* [2005] EWHC 3003 (QB), paras 135-137, stating at para 137: “People feel, and are entitled to feel, free in their homes to speak unguardedly and with less inhibition than in public places. Accordingly, it will be rare indeed that the public interest will justify encroaching upon such goings on.” See further Daniel Watterson “Privacy in the Home: A Critical Evaluation of Existing Protections” (LLB(Hons) Research Paper, Victoria University of Wellington, 2007).

intrusions in their homes does not extend to a right not to be observed casually by passers-by or by neighbours who are able to see into parts of a house. The law does, however, provide some protection against prolonged watching by making peeping and peering into a dwelling house at night an offence, and by making watching a person in that person's place of residence a "specified act" for the purposes of the Harassment Act. In our view, using a visual surveillance device to observe, record or monitor a person in his or her home is a serious interference with that person's right to privacy. The use of devices allows activities and objects to be focused on in close detail, and allows a record to be made of activities taking place in the home. This is quite different from casual observation with the naked eye. We think it is sufficiently intrusive that it should be covered by the criminal law.

3.36 In describing the new offence, we have used the term "dwelling" (rather than "house", "dwelling house" or "home") in order to indicate that the category of place we are talking about is not restricted to houses but is not so broad as to include all private premises. We think that the offence should apply to visual surveillance of the interior of any place in which a person lives, including places where a person lives temporarily, and in which a person has a reasonable expectation of privacy. The fact that such places often have multiple residents does not diminish the residents' reasonable expectations of privacy with respect to surveillance by non-residents. Dwellings are generally places within which people would be expected to sleep, bathe, and engage in other activities that would not normally be conducted in public. The places we have in mind include:

- private houses or apartments;
- rooms in hotels, motels, guesthouses, hostels, and similar places;
- rooms in homeless shelters, safe houses for survivors of domestic abuse, or other places of shelter or refuge;
- all buildings that form part of a marae (but not the open ground within the boundary of the marae);
- those parts of hospitals, nursing homes, hospices or similar places in which people reside and have sleeping accommodation, or receive treatment; and
- vehicles that are also places of residence, such as campervans or boats with sleeping quarters.

On the other hand, "dwelling" does not include private premises such as shops, offices or schools, or those parts of places such as hotels or hospitals that are not used for residential purposes (or treatment purposes in the case of hospitals). How the Act should provide for the coverage we have just described is a drafting issue, but we suggest that the Act could provide a definition of "dwelling" or another suitable term.⁷⁶

⁷⁶ See, for example, the definition of "residential premises" in Regulation of Investigatory Powers Act 2000 (UK), s 48(1) and 48(7)(b); definition of "dwelling" in Law Reform Commission of Ireland *Report on Privacy: Surveillance and the Interception of Communications* (LRC 57, Dublin, 1998) 120 [*Report on Privacy* LRC 57, Dublin, 1998]; definition of "private premises" in *The Regulation of Covert Surveillance* LRC Hong Kong, above n 64, 9.

- 3.37 We recommend that the offence should not apply to visual surveillance of the curtilage of a dwelling, such as a yard, garden or deck. The expectation of privacy outside the walls of a dwelling is lower than within it, and not so high as to justify criminal charges for infringing it. While some people have high fences around their sections and could be considered to have a reasonable expectation of privacy behind their fences, it seems wrong that they should enjoy the protection of the criminal law while those without fences do not. We also note that, depending on the circumstances, remedies for visual surveillance of yards may be available under the tort of nuisance, or under the Privacy Act or the Harassment Act (especially if those Acts are amended in ways which we propose in chapters 4 and 5).
- 3.38 The offence requires that the visual surveillance be of the interior of a dwelling. It would not be an offence to photograph or film the exterior of a house, even if people can, incidentally, be seen inside the house. The focus of any observation or recording with a visual surveillance device from outside must be on the interior of the dwelling. We do not think this distinction will be difficult to make in practice, although there may be some borderline cases in which the courts will have to judge whether the focus was on the interior or the exterior. The problem does not arise if the visual surveillance device is located within the dwelling.
- 3.39 The fact that the visual surveillance must be undertaken with the intention of observing, recording or monitoring the residents of the dwelling also acts as a control on the scope of the offence. A person who photographs a house because of an interest in architectural history will not have such an intention. Nor would something like Google Street View be caught by the offence: Street View focuses on the exterior of buildings, and neither Google nor its photographers are acting with the intention of observing, recording or monitoring the residents.⁷⁷ No offence will be committed, either, if the interior of a dwelling is filmed at a time when no one is ordinarily resident there: when a house is for sale and unoccupied, or a motel room is unlet, for example.
- 3.40 There is no requirement in the offence that the visual surveillance must involve observation or recording of “private activity”, however that term might be defined. Filming a person who is standing in plain view by the windows of his or her house would be an offence, so long as the focus is on the interior of the house and the filming is for the purpose of observing, recording or monitoring the residents. Nor is it necessary that the residents should actually be seen or recorded, or even that they are in the dwelling at the relevant time (so long as there are people ordinarily resident there). For example, the interior of the dwelling could be filmed while the residents are absent in order to discover information about them, or a camera could be left filming continuously in the hope that it will capture images of the residents. The surveillance must be conducted with the *intention* of observing, recording, or monitoring the residents; whether or not they are actually observed or recorded, and whether or not private information about them is obtained by means of the surveillance,

⁷⁷ Google Street View, which has been introduced in New Zealand, is an online service that provides 360-degree views of cities from street level: see discussion in New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, Wellington, 2008) 133.

is not relevant to determining if the offence has been committed. The extent of the intrusion into the residents' private lives can be reflected in sentencing, and in any civil remedies that may be awarded.

- 3.41 The offence will not be committed if the surveillance was undertaken with the express or implied consent of the lawful occupiers of the dwelling. Consideration will need to be given to whether the statute should include provisions specifying who is able to give consent in the case of dwellings with multiple occupants, and in the case of buildings such as hospitals where the controlling authority may be able to give consent without the consent of every occupant being required.
- 3.42 It should be a defence to this visual surveillance offence that the accused believed, on reasonable grounds, that at the material time the particular part of the dwelling that was subject to surveillance using a visual surveillance device was being used primarily as a place of work or business. It is not uncommon for parts of a dwelling to be used as a place of work or business: for example, a counsellor might have an office at home and see clients there. As we discuss in chapter 6, we do not propose any new statutory provisions to cover workplace surveillance, and we do not think the situation should be any different if a workplace happens to be located within a dwelling. There are also public interest considerations in relation to surveillance (particularly filming by the media) in workplaces and businesses that do not apply to dwellings.
- 3.43 We have considered whether there should be a general public interest defence. Given the narrowness of the offence we are recommending and the high level of privacy that people legitimately expect in homes and other dwellings, we have concluded that the defence should be limited to certain types of public interest that are proportionate to the level of intrusiveness involved in visual surveillance of the interior of a dwelling. We propose that it should be a defence that the accused believed, on reasonable grounds, that the surveillance was necessary:
- (a) for the protection of the health or safety of any person, or for the protection of public health or safety; or
 - (b) to provide evidence that an offence had been or was being committed or planned;
- and that the surveillance was no more extensive than reasonably necessary for those purposes.
- 3.44 One example of the kinds of visual surveillance to which the “protection of health or safety” defence would apply is filming in nursing homes or hospitals in order to expose poor conditions or mistreatment of residents or patients. There have been a number of incidents in New Zealand and overseas in which covert filming or photographing of nursing home residents has been undertaken by the media or others for this purpose.⁷⁸ We believe the protection of health or

78 For some examples see “Resthome Inquiry Sparks Privacy Complaints” (18 November 2009) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 18 November 2009); “Family of Woman Tied up Defend Rest Home” (18 November 2009) *Dominion Post* Wellington www.stuff.co.nz (accessed 18 November 2009); John Plunkett “Nurse Who Secretly Filmed for Panorama is Struck Off Register” (16 April 2009) *Guardian* www.guardian.co.uk (accessed 14 December 2009); *BKM Ltd v British Broadcasting Corporation* [2009] EWHC 3151 (Ch) Mann J.

safety defence would cover such situations, so long as there were reasonable grounds for undertaking the visual surveillance and the surveillance was no more extensive than reasonably necessary for the purpose.

- 3.45 There should be an exception to the offence for law enforcement officers acting in accordance with a warrant or emergency warrantless power, and further exceptions for law enforcement and intelligence agencies may also be needed.

RECOMMENDATION

- R7 The Surveillance Devices Act should include an offence of using a visual surveillance device to observe or record the interior of a dwelling with the intention of observing, recording or monitoring the people who reside there, knowing that such observation or recording is done without the consent (express or implied) of the lawful occupiers of the dwelling. In addition to appropriate exceptions for law enforcement and intelligence agencies, the following defences should be available:
- That the accused believed, on reasonable grounds, that at the material time the particular part of the dwelling that was subject to surveillance using a visual surveillance device was being used primarily as a place of work or business.
 - That the accused believed, on reasonable grounds, that the surveillance was necessary:
 - (a) for the protection of the health or safety of any person, or for the protection of public health or safety; or
 - (b) to provide evidence that an offence had been or was being committed or planned;and that the surveillance was no more extensive than reasonably necessary for those purposes.

Tracking

- 3.46 There are currently no tracking device offences in New Zealand, although there are provisions relating to warrants for the use of tracking devices in existing law and in the Search and Surveillance Bill.⁷⁹
- 3.47 The New Zealand Law Society and the Office of the Privacy Commissioner, as well as two individual submitters, supported the creation of a new offence targeting the covert use of tracking devices. The New Zealand Law Society commented that technology was moving fast in this area, and that tracking device offences had been introduced in Australia. Fairfax and Business New Zealand opposed the creation of a new offence, Business New Zealand commenting that tracking devices had legitimate commercial uses.

⁷⁹ Summary Proceedings Act 1957, ss 200A-200P; Search and Surveillance Bill 2009, no 45-1, cls 42(b), 44-56.

- 3.48 We believe that the Surveillance Devices Act should criminalise certain uses of tracking devices. By tracking devices, we mean devices capable of being used to determine the geographical location of a person or object. We recommend the creation of a new offence of *knowingly installing, using or maintaining a tracking device to determine the geographical location of a person or thing, knowing that the device is installed, used or maintained without the consent of the person, or of the person having lawful possession or control of the thing.*
- 3.49 The new offence would cover scenarios such as these:
- I keeps finding her ex-partner, J, turning up nearby when she is out in public, even though he should have no way of knowing where she is. The Police investigate and find a cellphone with a GPS (Global Positioning System) under the dashboard of her car. The phone not only allows J to record I's conversations in the car, but also allows him to know where the car is.⁸⁰
 - K suspects that her husband, L, is having an affair. She employs a private investigator, who secretly installs software on L's GPS-equipped cellphone, which allows the investigator to view the phone's location via an online mapping service.⁸¹
- 3.50 It is not an offence to track people by physically following them, although depending on the circumstances this could constitute offensive behaviour in a public place, intimidation or criminal harassment. We think tracking people by means of devices is qualitatively different from tracking them in person for several reasons. First, where a hidden tracking device is used, the person being tracked is unable to take any protective measures. While some very skilled individuals may be able to follow a person without being detected, most people probably cannot do so for a prolonged period of time. Secondly, devices allow people to be tracked much more easily than physical following and greatly increase the scope of tracking, allowing it to occur anywhere and at any time. Thirdly, modern tracking devices produce digitised information that can be stored, transferred, analysed and combined with other data very easily.
- 3.51 Covert tracking robs people of the ability to choose whether or not others know where they are at a particular time. It can reveal very private information: that a person visited an abortion clinic or a gay bar for example. (We recognise that levels of accuracy and precision of tracking devices vary, but the trend is towards ever-more precise information about the location of a person or thing.) In the most serious cases, being tracked may make people feel insecure, or may genuinely threaten their safety if it is done by a violent ex-partner, for example. We consider, therefore, that use of tracking devices to track people without their knowledge or consent is a sufficiently serious interference with their privacy, autonomy and security that it should generally be prohibited.

80 Based on a real incident in the United States: Marie Tessier "Hi-Tech Stalking Devices Extend Abusers' Reach" (1 October 2006) *Women's ENews* www.womensenews.com (accessed 30 October 2009).

81 See Mark Russell "Warning on Mobile Phone Tracking" (8 March 2009) *The Age* Melbourne www.theage.com.au (accessed 11 March 2009).

3.52 At the same time, we recognise that there are many legitimate and beneficial uses of tracking devices. Moreover, spatial information has been recognised as having significant economic utility and potential to contribute to productivity gains.⁸² Some of the legitimate uses of tracking devices would be covered by the defence discussed below, while others are covered by the way in which the proposed offence has been framed. The following situations would not be caught by the offence:

- A waste management firm installs GPS devices in its vehicles in order to better manage the productivity of its drivers and the use of its trucks. This would not be an offence because the company is the lawful owner of the trucks. It should also have notified its employees that the vehicles are tracked. So long as the tracking of vehicles is spelled out in workers' employment agreements or otherwise made clear to them when they commence work with the firm, they would probably be considered to have consented to the tracking.
- A company uses a device attached to its products to track their progress through the supply chain, from the factory through distribution networks to retail outlets. This would not be an offence because the company and its distribution agents are lawfully in possession or control of the products until they reach their final destinations.
- M's laptop computer is equipped with software which, when activated, can transmit information about the location at which the computer is connected to the internet.⁸³ When the laptop is stolen, M is able to pass this information on to the Police, who use it to catch the thief. It would not be an offence to track the laptop in this way, because the thief is in possession of the computer unlawfully.
- N is signed up to a service that allows N and her friends to share their locations with each other via their mobile phones. People must sign up to be part of the service, and can switch it on or off at any time. N is not committing an offence by tracking the movements of her friends, because they have consented to be part of the service.

Some of these situations could involve privacy issues, but the privacy issues in such cases are appropriately covered by the Privacy Act. For example, where employees are tracked they should be notified that information about their movements is being collected, and the collection of information about employees by means of tracking devices should not intrude unreasonably into their personal affairs.⁸⁴

3.53 We should also emphasise that, although the offence includes tracking things as well as tracking people, tracking things is only of concern because it can allow the people associated with those things to be tracked. We do not think the proposed offence would interfere with the tracking of commercial goods or livestock, for example, because such tracking would be done by or with the consent of the lawful owner. Nor would the offence apply to the tracking of wild

82 ACIL Tasman *Spatial Information in the New Zealand Economy: Realising Productivity Gains* (report prepared for Land Information New Zealand, Department of Conservation and Ministry of Economic Development, 2009).

83 Rhodri Marsden "Tracking the Technology Thieves" (4 November 2009) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 5 November 2009).

84 Privacy Act 1993, s 6, information privacy principles 3 and 4.

animals that have no owners. If it is considered necessary to make clear that the offence is concerned with the tracking of people, it could specifically provide that using a tracking device to determine the location of a thing is only an offence if it is done for the purpose of determining the location of a person.

3.54 As we have already said, the offence would not apply to tracking done with the consent of the person concerned, or of the person having lawful possession or control of the thing concerned. Tracking would be permitted by law enforcement officers acting under warrant or an emergency warrantless power, and an exemption might also be needed for the intelligence organisations. In addition, we think that it should be a defence to the tracking device offence that the use of the tracking device was necessary for the protection of the health, safety or wellbeing of any person, or for the protection of public health or safety, and was no more extensive than reasonably necessary for those purposes. This defence would cover situations such as:⁸⁵

- Use of tracking devices to monitor the movements of dementia patients, to make sure they do not wander off and get lost.
- Use by parents or guardians of tracking devices to monitor the location of their children when they leave the house.
- A hospital using radio frequency identification chips to track the movements of patients within the hospital.

Once again, situations such as these may raise issues under the Privacy Act, but should not be covered by criminal offences in our view. We think a general defence as outlined above should be sufficient, but more specific exceptions could be included in the Act if considered necessary.

RECOMMENDATION

R8 The Surveillance Devices Act should include an offence of knowingly installing, using or maintaining a tracking device to determine the geographical location of a person or thing, knowing that the device is installed, used or maintained without the consent of the person, or of the person having lawful possession or control of the thing. In addition to appropriate exceptions for law enforcement and intelligence agencies, it should be a defence to this offence that the use of the tracking device was necessary for the protection of the health, safety or wellbeing of any person, or for the protection of public health or safety, and was no more extensive than reasonably necessary for those purposes.

Interception

3.55 Interception offences are already included in the Crimes Act.⁸⁶ These offences originally covered the interception of private oral communications by means of a listening device. Amendments to the Crimes Act in 2003 extended the scope

85 K Michael, A McNamee and M G Michael *The Emerging Ethics of Humancentric GPS Tracking and Monitoring* (University of Wollongong, Faculty of Informatics – Papers, 2006) paras 6.1 and 6.2; Claire McEntee “Tracking System to Tag Patients” (12 October 2009) *Dominion Post* Wellington www.stuff.co.nz (accessed 12 October 2009).

86 Crimes Act 1961, ss 216A-216F.

of the interception provisions so that they now cover interception of private communications of all kinds (oral, written, or other) by means of an interception device. The prohibition on use of interception devices therefore includes interception of such things as emails and text messages.

- 3.56 In our issues paper, we raised a number of questions about possible reform of the interception provisions in the Crimes Act.⁸⁷ We asked whether:
- the definition of “private communication” should be clarified;
 - the participant monitoring exception to the interception offence should be reformed in any respect; and
 - there should be specific restrictions on the disclosure of information obtained through participant monitoring.

The issue of restrictions on disclosure of information obtained through interception is discussed later in this chapter.

- 3.57 Few submissions specifically responded to these questions. There was some support for clarifying the definition of “private communication”. In particular, the New Zealand Law Society supported clarification to avoid uncertainties about expectations of privacy concerning the use of emails, text messages and cellphone communications and noted that the inconsistencies between the interception offences and the computer misuse offences “made no sense”. The New Zealand Law Society supported reforming the participant monitoring rules along the lines of the New South Wales offence and stated that authorised outsider monitoring (discussed below) should not be allowed. TVNZ suggested that in some limited circumstances the media should be permitted to intercept private communications where this is in the public interest. One individual felt that participant monitoring should require a warrant. Some other submitters did not support reform of the participant monitoring rules. The Privacy Commissioner supported new limits on the disclosure of lawfully-intercepted communications.
- 3.58 We recommend that the provisions in the Crimes Act providing for interception offences⁸⁸ should be removed from that Act, and should form part of the Surveillance Devices Act. Some amendments should be made to the existing interception provisions, as discussed below.

RECOMMENDATION

- R9 The provisions in the Crimes Act providing for interception offences should be removed from that Act and included in the new Surveillance Devices Act.

87 Privacy Stage 3 issues paper, above n 38, 247-252.

88 Crimes Act 1961, ss 216A-216F.

Private communication

- 3.59 “Private communication” is a statutory term that has been used in New Zealand since 1978,⁸⁹ and is also a familiar term in the listening device offences of the majority of Australian states and territories. While the current definition, by virtue of its longevity, has acquired a degree of orthodoxy, it is not straightforward and its difficulties have been judicially noted.
- 3.60 The original scope of the definition was confined to oral communications. In 2003, the definition was expanded to include communications “in written form or otherwise”.⁹⁰ Judge Harvey (writing extra-judicially) explains that the change is directed to electronic communications such as email, as well as any other sort of communication.⁹¹ In contrast, in the Australian states and territories, the definition of private communication has not been expanded to include written and electronic communications. However, at Federal level, the offence of intercepting telecommunications includes both conversations and messages.⁹²

Rationalising the privacy expectation criteria

- 3.61 As noted in our issues paper, there are two aspects to the current definition of “private communication”:⁹³
- the inclusion of a communication where it is reasonably clear that at least one party intends the communication to be confined just to the parties to the communication;⁹⁴ and
 - the exclusion of the communication if the parties ought reasonably to expect that the communication may be intercepted by an unauthorised person.⁹⁵
- 3.62 These two elements contribute to the enquiry as to whether it is reasonable for the communication to be treated as private, and therefore within the scope of the interception offence. If there is an expectation of privacy (by applying the criteria), then it can be considered unreasonable for a person to use an interception device to intercept the communication, and any such interception will be an offence.

89 For discussion of the legislative history, see *Moreton v Police* [2002] 2 NZLR 234, paras 15-19.

90 Crimes Amendment Bill (No 6).

91 David Harvey *internet.law.nz* (2 ed, LexisNexis, Wellington, 2005) 242. See also the Explanatory Note to Supplementary Order Paper 2000 No 85.

92 Telecommunications (Interception and Access) Act 1979 (Cth), s 7. The New South Wales Law Reform Commission notes that it is probable that the interception of telecommunications is governed exclusively by Federal law: *Privacy Legislation in New South Wales* (NSWLRC CP3, Sydney, 2008) para 5.99.

93 Privacy Stage 3 issues paper, above n 38, 247.

94 One party may authorise the interception of the communication by an outsider without disqualifying the communication from being private, due to the definition of “party” in the Crimes Act 1961, s 216A(2)(b).

95 This has been interpreted to require that both parties must hold the expectation for the communication to be excluded from being a private communication: *Moreton v Police*, above n 89. See discussion in Privacy Stage 3 issues paper, above n 38, 247.

- 3.63 The first element assesses the subjective intention of each party, while the second element is an objective assessment of whether the communication is susceptible to interception.⁹⁶ It is the second criterion, in particular, that is difficult to interpret on its face, and reference to case law is needed for a full understanding of the scope of the definition. The appropriate interpretation of the second limb was considered by William Young J in *Moreton v Police*.⁹⁷ As discussed in our issues paper, his Honour specifically considered whether the second limb required an assessment of the *risk* of interception, or the *likelihood* of interception.⁹⁸ He confirmed that communications are disqualified from being private, and are therefore outside the scope of the interception offence, only where there is an actual likelihood or real possibility of interception, rather than a theoretical risk.⁹⁹ According to the case law, “mere suspicion” of interception is not enough to satisfy the objective test.¹⁰⁰
- 3.64 There are a range of situations in which people may hold reasonable suspicions that they could be under surveillance, including the interception of their private communications.¹⁰¹ Public figures or celebrities may reasonably suspect surveillance and interception due to public interest in their activities.¹⁰² However, there would likely need to be some additional factor or circumstances (such as the discovery of an interception device or other signs or notice of interception, surveillance or harassment) that point to a reasonable likelihood of interception, in order for an otherwise private communication to be disqualified.
- 3.65 As we noted in our issues paper, Judge Harvey in his extra-judicial writing has raised questions about whether cellphone communications and unencrypted email are considered to be private communications.¹⁰³ A submitter queried whether communications sent from or between WiFi networks would be considered to be private communications. In *Moreton v Police*, William Young J noted that while public awareness has developed over time that cellphone communications are not particularly secure, this does not automatically give rise to an expectation that any particular call will be intercepted.¹⁰⁴ While the method of communication used and public awareness of its security levels may not be determinative on their own, they will nevertheless be relevant to whether at

96 Hon J Bruce Robertson (ed) *Adams on Criminal Law* (loose leaf, Brookers, Wellington, Crimes Act, 1992) para CA216A.03 [*Adams on Criminal Law*].

97 *Moreton v Police*, above n 89, paras 22-23, 36; discussed in Privacy Stage 3 issues paper, above n 38, 247-248.

98 Noting that, while the statutory language could be read as supporting the first interpretation, this would give the definition such broad application that virtually no communications could be regarded as private.

99 See also *R v Cheung* (1995) 100 CCC (3d) 441.

100 *Adams on Criminal Law*, above n 96, para CA216A.03; Harvey, above n 91, para 4.9.3.

101 For example, where people are aware that they are under investigation by law enforcement or being pursued by a stalker, where an activity a person engages in is likely to attract the scrutiny of law enforcement, the media or other investigators, or where the personal circumstances of the person may render them susceptible to private surveillance, such as where the person has made an insurance claim, or is involved in legal proceedings, a hostile relationship breakdown or an extramarital affair.

102 For example, the interception of telephone conversations of members of the Royal Family: see Harvey, above n 91, 243. See also *Moreton v Police*, above n 89, para 69.

103 Harvey, above n 91, 242-243; Privacy Stage 3 issues paper, above n 38, 248.

104 *Moreton v Police*, above n 89, paras 31-33, 61-72.

least one of the parties has indicated a desire that the communication be confined to the parties, and to whether there is a reasonable expectation (by both parties) that the communication may be intercepted.

- 3.66 A further issue with the second element of the definition of “private communication” is that it makes the interception offence somewhat circular as a matter of logic. The second element of the definition of “private communication” means that a communication can be rendered non-private and therefore susceptible to lawful interception if there is a sufficient likelihood that the communication may be intercepted. While the objective criterion has, in light of the case law, a reasonably high threshold, we think it is unsatisfactory that the scope of the interception offence can turn on the likelihood of interception, an activity which the offence provision is purporting to regulate. The likelihood of a privacy encroachment (through interception) should not be determinative of the application of the privacy protection provided by the interception offence.
- 3.67 We have considered whether the definition could be simplified or streamlined. One question is whether both elements of the definition are necessary. An argument could be made that the first element of “private communication” is sufficient on its own. It could be said that the likelihood of interception under the second limb contributes to the circumstances in which a communication is made under the first limb. For example, a communication made where the parties should be aware that there is a likelihood of interception (for example, because they are using an insecure communication channel such as CB radio) may negate the parties’ desire to confine the communication to themselves. We note that the second “private communication” criterion is not a feature of the offence against the use of listening devices in South Australia, the Australian Capital Territory or Tasmania. However, it is a feature of the offence in New South Wales, Victoria, Western Australia, the Northern Territory, and Queensland, as well as in New Zealand.¹⁰⁵
- 3.68 The current definition of “private communication” can be viewed as a form of the “reasonable expectation of privacy” test. For example, the Explanatory Note to Supplementary Order Paper 2000, no 85, describing the 2003 amendments to the interception offence states that: “The main justification for the change is that all forms of private communication should have the same level of protection, where there is a reasonable expectation of privacy.” A further option, therefore, is to explicitly replace the two elements of the definition with a single objective test of whether one or both parties has a reasonable expectation of privacy in the communication.¹⁰⁶ This would encompass both of the current criteria as it would involve an assessment of the circumstances of the communication and whether the parties intended the communication to be private (on an objective basis), and would reverse the current reasonable expectation of interception criterion to assess instead whether there is a reasonable expectation of privacy in all the circumstances. The advantages of a single reasonable expectation of privacy test are that it would simplify the definition of “private communication” to just one test instead of two, and it would resolve the current logical difficulty with having the scope of the interception offence depend on an objective

¹⁰⁵ Crimes Act 1961, ss 216B, 312A.

¹⁰⁶ See, for example, the offence proposed in *Report on Privacy* LRC 57, Dublin, 1998, above n 76, para 9.12.

likelihood of interception. While the likelihood of interception could be taken into account under the reasonable expectation of privacy test, it would be one factor to be taken into account, rather than a controlling factor on its own.

- 3.69 It is conceivable that, in the circumstances, one party may have a reasonable expectation of privacy, while the other party or parties do not have such an expectation. We recommend that a communication should be categorised as private even if only one party has a reasonable expectation of privacy. We do not think that the lack of a privacy expectation by one party should negate the privacy expectation of another.
- 3.70 Adopting the reasonable expectation of privacy test would foster greater consistency with other areas of law where privacy enquiries are required. The “reasonable expectation of privacy test” is now established in the common law in various contexts, such as the privacy tort, and in relation to assessments of “unreasonable search and seizure” under section 21 of the Bill of Rights Act 1990.¹⁰⁷ The reasonable expectation of privacy test is used as a flexible balancing exercise in circumstances where it is not possible to exhaustively define privacy limits, and thus permits judicial interpretation to develop boundaries over time in response to particular cases. We think that the interception of private communications is an area where this approach is appropriate. Existing jurisprudence relating to reasonable expectations of privacy is not directed specifically at a criminal offence such as interception, and therefore the introduction of the test in this context would represent a new development. However, the existing case law relating to interception would continue to provide guidance as the proposed reform would essentially constitute a restatement of the existing criteria, rather than introduce a completely new test.
- 3.71 We have considered whether adoption of the reasonable expectation of privacy test in this context provides sufficient precision as to the scope of the criminal offence. A form of the test was proposed in the United Kingdom for a broader offence of surreptitious use of a surveillance device, but was never adopted.¹⁰⁸ The Hong Kong Law Reform Commission initially concluded that the test was unsuitable for inclusion in the criminal law, being insufficiently precise to constitute a criminal standard,¹⁰⁹ but the Commission subsequently changed its view and decided that the reasonable expectation of privacy test was suitable for inclusion in a surveillance offence.¹¹⁰
- 3.72 We think that the adoption of the reasonable expectation of privacy test in the specific context of the interception of communications will provide sufficient certainty and precision as to its scope. Whether the parties have a reasonable expectation of privacy in a communication is a more focussed enquiry than in other contexts, such as whether the parties had a reasonable expectation in being

107 Overseas jurisprudence relating to reasonable expectations of privacy is also an available resource. For example, United States tort law and Fourth Amendment case law, as well as decisions on section 8 of the Canadian Charter of Rights and Freedoms.

108 Rt Hon Kenneth Younger (chair) *Report of the Committee on Privacy* (Cmnd 5012, London, 1972) para 563.

109 Law Reform Commission of Hong Kong *Privacy: Regulating Surveillance and the Interception of Communications: Consultation Paper* (Hong Kong, 1996) paras 1.59-1.60.

110 *The Regulation of Covert Surveillance* LRC Hong Kong, above n 64, 18-20.

free from surveillance (as proposed by the Younger committee in the United Kingdom). While the test is open-ended in nature, and there will be questions about whether there is a reasonable expectation of privacy in certain circumstances, particularly as new communications technologies are adopted, we consider that the scope of the offence is sufficiently clear. The degree of sensitivity associated with communications privacy (as evidenced by the enactment of the interception offence) means that the privacy expectation in this area is relatively high.

- 3.73 We anticipate that the main areas of enquiry by the courts will be whether the actions of the parties disqualify their communication from being a private one, and whether any particular method of communication disqualifies a communication from being a private one. By “the actions of the parties”, we mean their conduct of the communication itself; for example, whether they are talking in a private room where they expect no one else can hear them, or talking loudly in a public place. We do not mean that the content of the communication, or the status or identities of the parties, should affect their reasonable expectations of privacy. For example, just because someone is a prominent celebrity whose life is the subject of intense media speculation, that does not mean that she should reasonably expect to have her telephone conversations secretly recorded.
- 3.74 Certainty and precision of the interception offence are also important to law enforcement. The scope of the interception offence (including its various exceptions)¹¹¹ sets the threshold for when interception warrants must be obtained by law enforcement officers who seek to intercept communications for law enforcement purposes. We are satisfied that the adoption of a reasonable expectation of privacy test would not create undue uncertainty for law enforcement agencies. This is, in part, on the basis that law enforcement agencies are already subject to and familiar with this test under section 21 of the Bill of Rights Act 1990.¹¹² We further note that where there is an area of doubt as to whether interception of a particular mode of communication in the absence of a warrant breaches reasonable expectations of privacy, law enforcement officers have the fall back options of (i) utilising the interception warrant regime, or (ii) utilising the exceptions to the interception offence, to ensure that any such interception is not unlawful.
- 3.75 On balance, we prefer the option of restating the two current criteria as a single objective reasonable expectation of privacy test.

111 For example, participant monitoring (Crimes Act 1961, s 216B(1)(a)); or emergency interception by law enforcement where there is a risk to life or of serious injury (Crimes Act, s 216B(3)).

112 While the White Paper that preceded the Bill of Rights Act contemplated that electronic interception and other forms of surveillance would be subject to section 21, the courts are yet to provide firm guidance on whether electronic surveillance such as the interception of private communications constitutes a “search” for purposes of section 21: see Ministry of Justice *Guidelines on the New Zealand Bill of Rights Act 1990: A Guide to the Rights and Freedoms in the Bill of Rights Act for the Public Sector* (Wellington, 2004); New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007) paras 11.34-11.37 [*Search and Surveillance Powers* NZLC R97].

RECOMMENDATION

R10 The definition of “private communication” for the purposes of the interception offences should be amended to replace the two current criteria with a single “reasonable expectation of privacy” test.

Expectations of privacy and different modes of communication

- 3.76 In the issues paper we asked whether the privacy-expectation enquiry should be retained as a generic requirement of the interception offence, or whether its application should be limited to particular types of communication. The ambulatory nature of the privacy-expectation enquiry suggests that there may be a case for limiting such enquiries only to particular forms of communication, to ensure that the scope of the interception offence is not overly broad.¹¹³ We asked whether the privacy expectation enquiry should be reserved for oral communications between people in person and discarded in relation to other forms of communication such as telephone calls, text messages and emails. Without the privacy-expectation enquiry, these forms of communication could be presumed to be private and protected from unauthorised interception.¹¹⁴
- 3.77 We discuss this issue further in Appendix A, but present our conclusions here. We consider that the reasonable expectation of privacy test is a necessary general element of the regulation of the interception of oral communications (whether in person, by telephone, or otherwise). In relation to the interception of electronic communications in written or other non-oral form, however, we conclude that the application of the reasonable expectation of privacy test requires further expert review and consultation. We also anticipate that confining the reasonable privacy expectation test to particular types of communication may be a difficult drafting exercise.
- 3.78 We therefore recommend that the review of data surveillance which we have recommended above should include an assessment of the adequacy of the current legal framework for the interception of electronic communications, including the suitability of the reasonable expectation of privacy test and consideration of the issues discussed in Appendix A.
- 3.79 Pending the outcome of the review of data surveillance, the definition of “private communication”, and the reasonable expectation of privacy test, should continue to apply to all forms of communication (“whether in oral or written form or otherwise”) that can be intercepted by means of an interception device.

¹¹³ Privacy Stage 3 issues paper, above n 38, 247-249.

¹¹⁴ However, other exceptions to the interception offence would continue to apply, such as the exception for interception warrants for law enforcement purposes (Crimes Act 1961, s 216B(1)(b)(i)).

RECOMMENDATION

R11 The review of data surveillance (see R3 above) should include an assessment of the adequacy of the current legal framework for the interception of electronic communications, including the suitability of the reasonable expectation of privacy test for different types of electronic communication, and consideration of the issues discussed in Appendix A.

Participant monitoring

- 3.80 As noted in our issues paper, participant monitoring is a significant exception to the interception offence.¹¹⁵ We also noted that there is a range of views as to the impact of participant monitoring on the privacy interests of a party to a communication who is unaware that an otherwise private communication is being monitored or recorded by another party or by an outsider authorised by one of the other parties.¹¹⁶ Nevertheless, it is clear that there are circumstances in which participant monitoring has a legitimate purpose and function in protecting both private and public interests. There are occasions when important public interests are served by permitting the parties and authorised outsiders to record and monitor private communications. Examples include investigative reporting by the media, members of the public protecting their own legal positions, and investigations by law enforcement agencies.¹¹⁷
- 3.81 As we outlined in the issues paper, there are two forms of participant monitoring:
- where one party records or otherwise intercepts a communication without the other parties' knowledge or consent (we called this form principal party monitoring); and
 - where one party authorises someone else to intercept a communication, without the other parties' knowledge or consent (we called this form authorised outsider monitoring).
- 3.82 The participant monitoring exception means that one party's privacy expectations can be overridden by the actions of another party to the communication. The interception might be done by a party to the communication for his or her own reasons (for example, to protect his or her lawful interests), or might be done at the instigation of a third party such as a law enforcement agency, the media or some other person with an interest in intercepting a communication with only one party's consent. It is the Commission's view, in line with the current law, that parties to private communications should not be limited by the criminal law from recording those communications for their own legitimate purposes, or authorising an outsider to record or intercept the communication for legitimate purposes. This is consistent with the Commission's view at the time of the report on *Search and Surveillance Powers*, which was that law

115 Privacy Stage 3 issues paper, above n 38, 249.

116 Ibid, 250.

117 Private investigators are prohibited from recording speech (whether or not part of a private conversation) without consent under the Private Investigators and Security Guards Act 1974, s 52.

enforcement agencies should be able to utilise both aspects of the participant monitoring exception.¹¹⁸ As noted in our issues paper, the privacy principles act as a limit on participant monitoring in certain circumstances.¹¹⁹

- 3.83 We have considered whether the participant monitoring exception should be subject to some statutory limitations, in addition to those imposed by the Privacy Act. We have reviewed the participant monitoring exceptions to the listening device offences in the Australian states and territories. All the Australian jurisdictions (except Queensland) express the participant monitoring exception as being subject to broad limitations, such as that participant monitoring is:
- reasonably necessary for the protection of a party's lawful interests;¹²⁰
 - in the public interest;¹²¹ or
 - conducted by a law enforcement officer in certain circumstances.¹²²
- 3.84 The breadth of these formulations likely renders most participant recordings lawful, and the adoption of such broad limits may not represent a major limitation on the participant monitoring exception. That being said, these broad formulations may be of value in clarifying that participant recordings made without justification are not defensible. Examples of cases where there may be insufficient legitimate justification for participant recording would include the recording of conversations for entertainment or exploitative purposes without the knowledge or consent of the person being recorded, or the recording of private conversations for the purpose of embarrassment, humiliation, retaliation or harassment. Participant monitoring for the purposes of blackmail or to threaten or inflict serious injury to the reputation or personal interests of one of the participants may be particularly harmful. One example would be the taping of conversations on sex chat lines in order to damage the reputations of public figures or the private lives of ordinary citizens, where there is no redeeming public interest.
- 3.85 Currently, the privacy principles regulate inappropriate participant monitoring, either through principle 4 (personal information shall not be collected by means that, in the circumstances of the case are unfair, or intrude to an unreasonable extent upon the personal affairs of the individual concerned), principle 10 (limits on use of personal information) or principle 11 (limits on disclosure of personal information). Where there is disclosure of the contents of a participant recording, there may also be a remedy under the *Hosking* privacy disclosure tort. The question is whether objectionable forms of participant monitoring, such as those referred to in the previous paragraph, should be criminalised.

118 *Search and Surveillance Powers* NZLC 97, above n 112, 328 (recommending that the existing statutory formulation should be retained with respect to interception warrants), 331 (recommending the retention of the participant monitoring exception with regard to conversations).

119 Privacy Stage 3 issues paper, above n 38, 251 (n 1055).

120 Surveillance Devices Act 2007 (NSW) (both forms of participant monitoring); Listening Devices Act 1972 (Tas) (both forms of participant monitoring); Listening Devices Act 1992 (ACT) (authorised outsider monitoring); Listening and Surveillance Devices Act 1972 (SA) (principal party monitoring).

121 Surveillance Devices Act 1998 (WA) (both forms of participant monitoring); Listening and Surveillance Devices Act 1972 (SA) (principal party monitoring).

122 Surveillance Devices Act 2007 (NSW) (both forms of participant monitoring); Surveillance Devices Act 1999 (Vic) (authorised outsider monitoring); Surveillance Devices Act 1998 (WA) (authorised outsider monitoring); Surveillance Devices Act 2007 (NT) (authorised outsider monitoring).

- 3.86 We recommend that both forms of the participant monitoring exception to the interception offence be retained, but that limits should be placed on it to enable harmful uses to be dealt with. We think that there is merit in broadly stating the purposes for which participant monitoring may be undertaken, drawing on the Australian participant monitoring exceptions, so that there can be greater confidence that monitoring can be used only for legitimate purposes. The grounds we recommend are:
- where participant monitoring is reasonably necessary for the protection of the lawful interests of one or more of the principal parties to the communication;
 - where there are reasonable grounds to believe that participant monitoring is in the public interest; and
 - where participant monitoring is carried out by a law enforcement officer acting in the course of duty.
- 3.87 We take a broad view of the “protection of lawful interests” purpose. It would include, for example, the recording of a telephone interview by a member of the news media for the purpose of ensuring an accurate account of the interview in a news report. It would also include a recording made by any participant in a conversation when it is important to keep a more accurate record than memory may be able to provide.
- 3.88 Another way of achieving the same end might be to qualify the lawfulness of participant monitoring by spelling out an appropriately framed exception.¹²³ However, an exception to participant monitoring would be difficult to draft, and may be unduly complex, as participant monitoring is itself an exception to the interception offence. We think that a broad statement of the purposes for which participant monitoring may be undertaken is preferable.
- 3.89 It should be noted that the proposed reform is limited to the treatment of participant monitoring under the criminal law and under the right of civil action to be included in the Surveillance Devices Act. Other remedies that may be available as a matter of civil law, such as Privacy Act remedies, would not be affected by these proposals.
- 3.90 We also recommend in chapter 6 that the express restriction on private investigators recording voices or speech should be repealed, so that private investigators may make any such recordings, provided that they do not commit interception offences. This would put private investigators on the same footing as other sectors such as the media, and the general public.
- 3.91 We suggest that neither form of participant monitoring should be an exception to the interception of electronic communications such as email and text messages. The nature of this method of communication involves the production of a message that can be retained by the recipient, rendering principal party monitoring superfluous. If a principal party wishes to circulate the message to

¹²³ See for example 18 USC § 2511(2)(d): “It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral or electronic communication where such party is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.”

outsiders, that can be done by forwarding any message after it is received, without needing to authorise the interception of the message by the outsider. However, we think that this issue should be included in the recommended review of data surveillance.¹²⁴

RECOMMENDATION

- R12 Participant monitoring of private communications (both principal party monitoring and authorised outsider monitoring) should be permitted where:
- it is reasonably necessary for the protection of the lawful interests of one or more of the principal parties;
 - there are reasonable grounds to believe that monitoring is in the public interest; or
 - the participant monitoring is conducted by a law enforcement officer acting in the course of duty.

RECOMMENDATION

- R13 Further consideration should be given to whether participant monitoring should be a permitted exception to the interception of non-oral electronic communications.

SECONDARY CRIMINAL OFFENCES

- 3.92 In addition to the primary offences discussed above, we recommend that the Surveillance Devices Act should provide for two further offences of disclosing material obtained by unlawful surveillance, and selling or supplying surveillance devices or software. These offences would reinforce the primary offences, as we discuss below.

Disclosure

- 3.93 The Crimes Act already contains prohibitions on the disclosure of unlawfully-intercepted private communications, and on publication of intimate visual recordings.¹²⁵ It is also an offence for a person to knowingly disclose a private communication intercepted lawfully under warrant or emergency permit, otherwise than in the performance of that person's duty.¹²⁶ The disclosure, otherwise than in performance of a person's duty, of material obtained lawfully in the exercise of a surveillance power is to be prohibited by the Search and Surveillance Bill,¹²⁷ and does not concern us here.
- 3.94 We think it should be an offence for a person *to disclose information (including images and recordings) if that person knows, or ought reasonably to know, that the information was obtained directly or indirectly by the use of a surveillance device in*

124 For discussion of the issues associated with parties consenting to surveillance in the context of the internet, see Orin S Kerr "Internet Surveillance Law After the USA Patriot Act: the Big Brother That Isn't" (2003) 97 Northwest U L Rev 607, 662-665.

125 Crimes Act 1961, ss 216C, 216J.

126 Ibid, s 312K.

127 Search and Surveillance Bill 2009, no 45-1, cl 171.

contravention of the criminal provisions of the Act. Whether this would be a single offence or whether separate disclosure offences would be needed for each primary offence is a drafting matter that we need not decide here.

- 3.95 The disclosure offence would thus directly mirror the primary offence: if it is an offence to undertake the surveillance, then it is also an offence for anyone to disclose information obtained by means of that surveillance. This would help to prevent the harm of the original surveillance from being made worse by revealing private information about a person, information that in all probability could not have been obtained without the use of a surveillance device.
- 3.96 We have considered whether there should be any departures from the basic principle that the disclosure offence should mirror the primary offence. There are two questions that need to be considered:
- Are there any circumstances in which it should be an offence to disclose information that was obtained lawfully by the use of a surveillance device?
 - Are there any circumstances in which it should be lawful to disclose information even though it was obtained by unlawful surveillance?

Disclosure of lawfully-obtained information

- 3.97 As noted in our issues paper, most of the Australian states and territories impose some form of restriction on the publication of lawfully-intercepted communications. These restrictions have the effect of controlling the use that can be made of material obtained through participant monitoring.¹²⁸ We have recommended above that broad limits should be placed on the participant monitoring exception to the interception offence. Such limits would have the effect of making participant monitoring of private communications beyond certain broad purposes unlawful. Consequentially, section 216C of the Crimes Act, or the proposed disclosure offence under the Surveillance Devices Act, would render the disclosure or publication of private communications unlawful if they were obtained by participant monitoring that was not undertaken for one of the permitted purposes. Beyond this, in relation to participant monitoring we recommend no departure from the principle that it should not be an offence to disclose material that has been lawfully intercepted. Disclosure of information obtained through participant monitoring could still be subject to civil remedies, such as under the Privacy Act or the tort of invasion of privacy, in some circumstances.
- 3.98 We have considered whether internet service providers and communication service providers should be restricted from disclosing or publishing private communications that are intercepted for the purpose of maintaining the internet or other communication service. Section 216B(5) of the Crimes Act provides that persons providing an internet or other communication service to the public may lawfully intercept private communications if the interception is carried out by an employee in the course of that person's duties; the interception is carried out, and is necessary, for the purpose of maintaining the internet or other communication service; and the interception is only used for the purpose of maintaining the internet or other communication service. Providers relying on

¹²⁸ Privacy Stage 3 issues paper, above n 38, 251.

this exception must destroy information obtained under subsection (5) immediately if it is no longer needed for the purpose of maintaining the service.¹²⁹ The Crimes Act currently prohibits disclosure of any information obtained when undertaking maintenance of a communication service,¹³⁰ but the relevant section (which also deals with unlawful disclosures relating to interception warrants) is to be repealed by the Search and Surveillance Bill.¹³¹ We recommend that it should continue to be an offence to disclose information lawfully obtained by providers of internet and other communication services when undertaking maintenance of those services. Communication service providers are allowed to intercept private communications only for a very specific purpose, and it would be an abuse of that licence if they were then permitted to disclose those communications for another purpose.

- 3.99 We have also considered the exception to the interception offence for the monitoring of prisoner calls and are satisfied that the statutory regime in the Corrections Act 2004 provides adequate controls.¹³²
- 3.100 In relation to forms of surveillance other than interception, and assuming the continuation of restrictions on disclosure of information obtained in the exercise of a law enforcement surveillance power, we can think of no cases in which it should be a criminal offence to disclose information that was obtained lawfully.

Disclosure of unlawfully-obtained information

- 3.101 It could be argued that there may be some cases in which it should be lawful for information to be disclosed in the public interest, or for the protection of lawful personal interests, even though it was obtained unlawfully. We cannot see a good case for such exceptions, however. Allowing the disclosure of information obtained unlawfully would simply encourage the circumvention of the law: a person could obtain embarrassing information about a celebrity by means of unlawful visual surveillance, for example, and then pass that information on to the media, who might be able to argue that they are free to publish it in the public interest. If there are good reasons for allowing certain types of surveillance (such as protection of health and safety) then they should be provided for in the primary offence; setting up different criteria for the primary offence and the disclosure offence is not desirable.
- 3.102 A few specific exceptions will be needed for the disclosure offence, however. In particular, it should not be an offence to disclose information to a person who is a subject of the surveillance (a party to a private communication, a person who has been filmed by a visual surveillance device, or a person whose movements have been tracked using a tracking device), or with the consent of the subjects of the surveillance. It should also not be an offence to disclose information for purposes such as a Police investigation or legal proceedings concerning an alleged surveillance offence.

129 Crimes Act 1961, s 216B(6).

130 Ibid, s 216F(1)(b)(i).

131 Search and Surveillance Bill 2009, no 45-1, cl 297(5).

132 Corrections Act 2004, ss 111-122. Disclosure is limited to the purposes for the monitoring, the Privacy Act expressly applies to monitoring and provision is made for destruction of monitored calls.

RECOMMENDATION

R14 The Surveillance Devices Act should make it an offence for a person to disclose information (including images and recordings) if that person knows, or ought reasonably to know, that the information was obtained directly or indirectly by the use of a surveillance device in contravention of the criminal provisions of the Act.

RECOMMENDATION

R15 It should continue to be an offence for a provider of internet or other communication services to disclose information obtained by intercepting private communications when undertaking maintenance of a communication service.

Sale, supply and related matters

- 3.103 The Crimes Act currently includes a prohibition on sale and supply of interception devices in certain circumstances, and on making, selling, distributing or possessing software for accessing a computer without authorisation for the purpose of committing a crime.¹³³ We think there should be similar offences in the Surveillance Devices Act, but they should be very tightly drawn and restricted to cases in which a person is clearly aiding or encouraging the commission of a crime. It would be impossible to outlaw all devices that can be used to conduct unlawful surveillance, as most of them have entirely legitimate uses. Knowingly promoting the illegal use of surveillance devices should, however, be outlawed.
- 3.104 We recommend that it should be an offence *to make, sell or supply a surveillance device, or software that can convert a device into a surveillance device, knowing that the device or software is to be used to undertake surveillance in contravention of the criminal provisions of the Surveillance Devices Act; or to promote or hold out a device or software as being useful for the carrying out of surveillance in contravention of the Act*. Thus, it would not be an offence to sell or supply a surveillance device if the person so doing did not know that the device was to be used to commit an offence under the Act. It would, however, be an offence for a private investigator to supply a client with a tracking device, knowing that the client intended to install it in the car of his ex-partner for the purpose of tracking her.

RECOMMENDATION

R16 The Surveillance Devices Act should provide that it is an offence to make, sell or supply a surveillance device, or software that can convert a device into a surveillance device, knowing that the device or software is to be used to undertake surveillance in contravention of the criminal provisions of the Surveillance Devices Act; or to promote or hold out a device or software as being useful for the carrying out of surveillance in contravention of the Act.

¹³³ Crimes Act 1961, ss 216D, 251.

- 3.105 The Surveillance Devices Act should provide for a civil right of action for breaches of any of the criminal provisions (including what we have described as the secondary offences). Damages and other standard tort remedies should be available if it can be proved to the civil standard (on the balance of probabilities) that one of the criminal provisions of the Act has been breached.
- 3.106 The right of action should be available to any person, including a legal person. We can see no reason why a corporation should not be able to sue if, for example, its board room has been bugged. Some of the offences will not, by their nature, apply to corporations – corporations do not have “dwellings”, nor do they have bodies that can be intimately filmed, for example – but where the offence can be committed against a corporation, the civil remedy should also be available to corporations.
- 3.107 The same defences should be available for a civil action as are available for the relevant offence. We considered whether a broader defence of “legitimate public concern” should be available for the civil action, in order to maintain consistency with the *Hosking* tort. On balance, however, we think the specific defences for each offence are also adequate for the civil action, given the reasonably tightly-focused nature of the offences.

RECOMMENDATION

R17 The Surveillance Devices Act should provide for a right of civil action by any person affected by a breach of any of the criminal provisions. Standard tort remedies should be available, and the defences should be the same as for the relevant offence.

Chapter 4

The Privacy Act 1993 and surveillance

- 4.1 As we discussed in chapter 1, the Privacy Act 1993 is the subject of stage 4 of the Law Commission’s Review of Privacy. Our review of the law relating to surveillance would be seriously incomplete, however, if we did not consider the role of the Privacy Act in regulating surveillance. In many respects the regulation of surveillance by means of the Privacy Act is working well, and we indicate in this chapter some areas which we think are best regulated within the framework of the Act. We also discuss some issues concerning the Privacy Act’s application to surveillance, and some ways in which we think the Act should be reformed to improve its coverage of surveillance. Our ideas for reforms to the Privacy Act with regard to surveillance will be carried through into stage 4 of our Review, and we will seek submissions on proposed reforms to the Act in our issues paper for that stage.

THE ROLE OF THE PRIVACY ACT IN REGULATING SURVEILLANCE

- 4.2 To the extent that surveillance involves the collection of personal information, it must comply with the Privacy Act. The Privacy Act provides a principles-based framework for regulating the way in which personal information is collected, held, used and disclosed. It also provides for a number of exceptions and exemptions to the privacy principles set out in the Act. In addition, the Privacy Act establishes the Privacy Commissioner as an independent watchdog on privacy issues. The Privacy Commissioner can hear complaints about breaches of the privacy principles, and can also make statements, undertake research and inquire into matters relating to the privacy of the individual. The Privacy Act can thus play an important role as a mechanism for dealing with complaints and providing remedies in relation to surveillance that breaches the privacy principles. The Privacy Commissioner can also play a general oversight role, and alert the government and society to developments in surveillance that may threaten privacy.
- 4.3 There was a clear consensus in the submissions we received that the Privacy Act should apply to surveillance, and a significant amount of support for clarifying the Act’s application to surveillance through amendments to the Act. We discuss possible amendments to the Act to improve its coverage of surveillance later in this chapter.

Are separate surveillance principles or a surveillance regulator needed?

- 4.4 While the Privacy Act can be a very effective tool for the regulation of surveillance, it is not a perfect fit. The privacy principles in the Act are focused on informational privacy, whereas surveillance can also be a major intrusion into spatial privacy.¹³⁴ Furthermore, the harms that can be caused by surveillance (especially mass surveillance systems) go beyond invasion of privacy. They include harms relating to issues of power and social control; in particular, profiling of people based on characteristics such as ethnicity or age and discrimination based on such profiling.¹³⁵
- 4.5 In our issues paper we raised the possibility of a new set of surveillance principles, either in the Privacy Act or in a new surveillance statute. A set of principles for the regulation of overt surveillance was proposed by the New South Wales Law Reform Commission, although their proposal has not been implemented.¹³⁶ There was little support in submissions for separate surveillance principles, and most submitters felt that the existing privacy principles could deal adequately with surveillance (although they might need some modification). We agree that new principles for dealing with surveillance are not needed. We think that, with some amendments discussed below, the existing privacy principles can deal effectively with most routine forms of surveillance. The Privacy Commissioner and Human Rights Review Tribunal have dealt with a number of complaints involving surveillance,¹³⁷ as have comparable bodies overseas. The Surveillance Devices Act that we discuss in chapter 3 would be available to deal with those types of surveillance that involve the most serious invasions of privacy. The Surveillance Devices Act would provide for a right of civil action, and would thus provide another avenue for seeking remedies for certain types of surveillance. We therefore see no need to complicate matters further by introducing a new set of principles to regulate surveillance.
- 4.6 Another option raised by the Victorian Law Reform Commission (VLRC) in its consultation paper on surveillance in public places is the creation of an independent regulator with responsibility for monitoring public-place surveillance.¹³⁸ The role of such a regulator could involve monitoring the use of surveillance, monitoring the operation and effectiveness of the law, informing people about how to comply with the law, promoting observance of best-practice standards, and reporting regularly to Parliament about the adequacy

134 On the distinction between informational and spatial (or local) privacy, see New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, Wellington, 2008) 57-60 [Privacy Stage 1 NZLC SP19].

135 Ibid, 47-48; New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington 2009) 204 [Privacy Stage 3 issues paper].

136 Privacy Stage 3 issues paper, above n 135, 256-257.

137 See for example the cases discussed in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 6.7(e), 202,404-202,410.

138 Victorian Law Reform Commission *Surveillance in Public Places* (VLRC CP7, Melbourne, 2009) 141-146 [*Surveillance in Public Places* VLRC CP7].

of surveillance regulation. Although the surveillance regulator would be a new and separate role, the VLRC noted that the Privacy Commissioner would be an obvious choice to exercise this role.

- 4.7 We do not see a need in New Zealand for a specific regulator to monitor surveillance. We do, however, believe that the Privacy Commissioner should carry out the roles proposed by the VLRC in relation to surveillance. The Commissioner can and does perform these roles already under her general functions set out in section 13 of the Privacy Act. For example, as discussed further below, the Commissioner has produced guidelines on privacy and Closed-Circuit Television (CCTV). However, we think it would be a good idea if the Privacy Act empowered the Privacy Commissioner to report regularly (perhaps every year, or every two years) to Parliament on developments in surveillance and surveillance technologies, and their implications for New Zealand. This would ensure that an independent agency is monitoring the growing potential of surveillance, and regularly bringing issues concerning surveillance to public attention. As part of this reporting function, the Privacy Commissioner could report on the operation and effectiveness of the Surveillance Devices Act, and on whether any amendments to the Act are required as a result of technological developments or other factors.
- 4.8 One person who commented on the Commission's online consultation website also suggested that surveillance measures should be subject to random audits, which could be carried out by the Privacy Commissioner. This person said that the key to achieving an acceptable balance between the benefits of surveillance and the protection of privacy is that those who use surveillance measures must be accountable and must be trusted.¹³⁹ We agree. In our issues paper on the Privacy Act we will be putting forward the idea of an expanded auditing power for the Privacy Commissioner, which would allow the Commissioner to undertake self-initiated audits of agencies. If such a power were to be included in the Privacy Act, it could be used to audit agencies using CCTV or other surveillance systems.

RECOMMENDATION

R18 The Privacy Act should provide that one of the functions of the Privacy Commissioner is to report regularly to Parliament on developments in surveillance and surveillance technologies, and their implications for New Zealand.

Regulation of specific types of surveillance: CCTV and RFID

- 4.9 In relation to some types of surveillance that were discussed in our issues paper, we have concluded that the Privacy Act is the most appropriate regulatory framework. This is the case in relation to CCTV and Radio-Frequency Identification (RFID), discussed below. It is also the case in relation to workplace surveillance, although such surveillance is governed by employment law as well as by the Privacy Act. We discuss workplace surveillance in chapter 6.

¹³⁹ Dominique, comment on www.talklaw.co.nz website, 29 July 2009. Auditing of CCTV is proposed in Siobhan Cervin "Closed-Circuit Television in New Zealand" (2009) 15 Auckland UL Rev 42, 73.

CCTV

- 4.10 CCTV looms large in any discussion of surveillance, and with good reason. It has become one of the most widely-used forms of mass surveillance, and its use continues to grow both overseas and in New Zealand. Even in the period since we released our issues paper, several cities and towns in New Zealand have introduced CCTV systems or expanded their existing systems.¹⁴⁰ CCTV is also widely used by businesses in New Zealand to protect the security of their property and employees. There is a widespread belief that CCTV makes communities safer, although the evidence of CCTV's effectiveness in deterring (as opposed to detecting and prosecuting) crime is not particularly strong.¹⁴¹ At the same time, CCTV can be used to collect large amounts of information about people's movements and activities, and thus clearly has significant implications for privacy. Advances in technology are greatly increasing the capability of users to capture and analyse personal information using CCTV.¹⁴²
- 4.11 In our issues paper we canvassed a number of options for the regulation of CCTV, including specific legislation dealing with CCTV, a code of practice or guidelines issued by the Privacy Commissioner, and the development of policies or best-practice standards for CCTV.¹⁴³ There was little support in submissions for a specific CCTV statute, and most submitters considered that CCTV should be regulated under the Privacy Act, perhaps with the assistance of guidelines or a code of practice issued by the Privacy Commissioner. Since we released our issues paper, the Privacy Commissioner has produced a guidance document for agencies in the public and private sectors that are currently using CCTV or considering the installation of CCTV systems. This guidance, which deals with non-covert CCTV systems in public and semi-public areas, is intended to assist agencies to use CCTV in ways that protect individual privacy and comply with the Privacy Act.¹⁴⁴
- 4.12 We believe the Privacy Act is the most appropriate regulatory framework for CCTV. While there are a range of concerns about CCTV, most of them boil down to a concern about the ways in which CCTV is used to collect personal information, and about how the personal information that is collected is stored, who has access to it, how long it is retained for, and how it is used and disclosed. These are all core Privacy Act issues. The Privacy Act provides a framework within which the perceived benefits of CCTV can be obtained while at the same

140 Wellington: Dave Burgess "More Cameras to Keep Eye on City Streets" (25 May 2009) *Dominion Post* Wellington www.stuff.co.nz (accessed 25 May 2009); Christchurch: Ian Steward "New Cameras Monitor City's Crime Hotspots" (22 May 2009) *The Press* Christchurch www.stuff.co.nz (accessed 22 May 2009); Panmure (Auckland): Melanie Verran "Cameras on Crims" (26 June 2009) *East & Bays Courier* www.stuff.co.nz (accessed 26 June 2009); Alexandra: "Alexandra CCTV to be Expanded" (21 July 2009) *Southland Times* 3; Taupo: "Taupo a Safer Place with CCTV Camera Network" (21 October 2009) Press Release, www.scoop.co.nz (accessed 21 October 2009); Newmarket (Auckland): Michael Dickison "Cameras Scaring Away Criminals" (27 October 2009) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 27 October 2009).

141 Privacy Stage 3 issues paper, above n 135, 197; *Surveillance in Public Places* VLRC CP7, above n 138, 82-84.

142 Privacy Stage 3 issues paper, above n 135, 190.

143 *Ibid.*, 259-262.

144 Privacy Commissioner *Privacy and CCTV: A Guide to the Privacy Act for Businesses, Agencies and Organisations* (Office of the Privacy Commissioner, Wellington, 2009) [*Privacy and CCTV*].

time protections can be put in place against the possible threats to privacy. CCTV differs from the more intrusive forms of visual surveillance that we believe should be covered by criminal offences under the Surveillance Devices Act (although if CCTV were to be used to conduct intimate covert filming or visual surveillance of the interior of a dwelling, an offence under the Surveillance Devices Act would be committed).¹⁴⁵ It is used in public and semi-public places where people's expectations of privacy are lower than in private places; it is not usually covert, because the cameras can be seen and ideally there will be signs in place notifying people that the area is under surveillance; and it is not targeted at particular individuals. There are still legitimate privacy concerns about CCTV, but these can be adequately dealt with under the Privacy Act.

- 4.13 In addition, some media organisations expressed concerns to us about the possibility that the media might be restricted from using CCTV images. Because the news media are excluded from the coverage of the privacy principles, if CCTV is left to be regulated under the Privacy Act there will be no change to the media's ability to use CCTV images. Complaints about media use of CCTV images can still be brought to the Press Council or the Broadcasting Standards Authority if such use breaches those bodies' principles and standards.
- 4.14 We think the issuing by the Privacy Commissioner of guidance on the use of CCTV is a very positive development, and that the guidance should be a very useful tool for agencies that wish to understand how CCTV can be used in ways that comply with the Privacy Act. It is now important to wait and see how agencies make use of that guidance. If guidance alone does not prove effective in controlling CCTV surveillance and ensuring that privacy is protected, the logical next step would be to develop a code of practice for CCTV under section 46 of the Privacy Act. A code of practice may, among other things, prescribe how the privacy principles are to be applied or complied with in relation to "any specified activity or class or classes of activities".
- 4.15 We have rejected more far-reaching suggestions for some form of authorisation or licensing of CCTV systems as impractical and overly bureaucratic.¹⁴⁶ It would be unrealistic to expect that such a requirement could ever be extended to all CCTV systems; it would probably be limited to public CCTV systems (such as those operated by local authorities) and perhaps some larger private users. This would mean that the great bulk of CCTV systems employed in small businesses and other private premises would not be covered by the licensing requirement, despite the fact that systems in such places can also give rise to privacy concerns. Licensing or authorisation would also impose a significant burden on whatever agency was responsible for administering the authorisation

145 See for example the case of two council CCTV operators in the United Kingdom who were convicted for training a street camera on a woman's flat and filming her while she was naked: "Peeping Tom CCTV Workers Jailed" (13 January 2006) www.bbc.co.uk (accessed 11 December 2009).

146 A requirement for authorisation of public CCTV systems is recommended in Cervin, above n 139, 71-73. The Victorian Law Reform Commission put forward licensing of certain types of surveillance systems, including CCTV, as an option in their consultation paper, and gave some examples from other jurisdictions: *Surveillance in Public Places* VLRC CP7, 150-151. The Republic of Ireland provides for the authorisation by the Garda Commissioner (Commissioner of Police) of the installation and operation of CCTV systems for the purpose of securing order and safety in public places: Garda Síochána Act 2005 (Republic of Ireland), s 38.

process, as well as on those agencies that would be required to have their systems authorised. Nor do we believe that such a requirement would significantly check the growth of CCTV systems, as we think that permission to install CCTV would seldom be refused. At best, it would be a mechanism for ensuring compliance with the existing requirements under the Privacy Act.

- 4.16 There is, however, a licensing requirement already in place in New Zealand law which we believe could be used to help ensure that CCTV is operated in a way that protects privacy. Under the Private Investigators and Security Guards Act 1974, security guards and their responsible employees are required to be licensed (or issued with certificates of approval, in the case of employees). “Security guard” is defined as meaning, among other things, a person who carries on a business that involves installing, operating, repairing, removing, selling, advising on or monitoring, on premises not owned or occupied by that person, a camera or similar device for the purpose of detecting the commission of offences on those premises.¹⁴⁷ The Private Security Personnel and Private Investigators Bill currently before Parliament has similar licensing requirements. The Bill covers a wider range of occupational classes, and there are several occupations covered by it whose work involves installing and repairing, selling and advising on, and monitoring of security cameras respectively: security technicians, security consultants and property guards.¹⁴⁸
- 4.17 The Private Investigators and Security Guards Act provides for the making of regulations prescribing codes of ethics for security guards and their responsible employees, and there is a similar provision in the Private Security Personnel and Private Investigators Bill.¹⁴⁹ The Bill also makes provision for the making of regulations prescribing training that applicants for licenses or certificates of approval are required to complete.¹⁵⁰ We believe these mechanisms should be used to ensure that private security personnel who install, advise on, operate and monitor CCTV systems are aware of legal and ethical requirements in relation to privacy. A code of ethics should be made under the current Act or any replacement statute, and should cover the privacy standards that private security personnel are required to meet in relation to CCTV systems. Any prescribed training should also cover privacy issues relating to CCTV, including legal obligations under the Privacy Act and other relevant legislation. If our recommendation for a Surveillance Devices Act were to be implemented, CCTV installers would need to know that it is an offence to install a surveillance camera on private premises where such installation involves entry to the premises without the consent of the lawful occupier, for example. We note that the New Zealand Security Association, a body representing the security industry, already has a code of practice in relation to CCTV systems which includes some coverage of legal requirements relating to privacy,¹⁵¹ but this code

147 Private Investigators and Security Guards Act 1974, s 4(1)(c)-(e).

148 Private Security Personnel and Private Investigators Bill 2008, no 297-1, cls 6, 7, 9.

149 Private Investigators and Security Guards Act 1974, s 71(h); Private Security Personnel and Private Investigators Bill 2008, no 297-1, cl 106(1)(l).

150 Private Security Personnel and Private Investigators Bill 2008, no 297-1, cl 106(1)(g).

151 New Zealand Security Association *Code of Practice: Closed Circuit Television Surveillance Systems* (version 4, November 2006) especially paras 2.1.1, 2.1.3-2.1.5, 2.3, 4.2.

does not have any legal force. There are also New Zealand Qualifications Authority unit standards relating to the design and installation of CCTV systems, but they do not appear to include coverage of privacy requirements.¹⁵²

- 4.18 Unlike in the United Kingdom,¹⁵³ it appears that in New Zealand operators of CCTV systems in public places (such as local council systems) are not required to be licensed or trained. Nor is there any requirement for people who use CCTV systems on their own premises to be licensed. The Privacy Commissioner's CCTV Guidelines, however, state that all agencies that operate CCTV systems should provide training for staff and ensure that staff are aware of the need to protect people's privacy.¹⁵⁴ While provision of such training is not itself a legal requirement, it is an essential part of ensuring that the requirements of the Privacy Act and other legislation are complied with. For example, Wellington City Council requires that staff undergo training before they are allowed to monitor CCTV cameras, and this training includes briefings on ethics and the Privacy Act.¹⁵⁵ We would hope that other local authorities also require operators of CCTV systems to undergo such training.

RFID

- 4.19 We described RFID technology in our study paper for stage 1 of this Review.¹⁵⁶ It has many practical and beneficial applications, particularly in identifying and storing information about goods as they make their way along supply chains. However, there are also privacy concerns about the potential to use RFID chips to identify and track people, and about the security of personal information stored on chips in documents such as passports. RFID technology is not yet in widespread commercial use in New Zealand, but a voluntary RFID Consumer Protection Code of Practice has been developed for New Zealand by an industry body.¹⁵⁷ In our issues paper we asked whether any specific regulatory measures were needed for RFID.¹⁵⁸ There was no consensus on this question in the submissions we received.
- 4.20 As we indicated in our issues paper, it is probably premature to establish a mandatory regulatory framework for RFID in New Zealand at present. We think it is important to monitor international developments in RFID regulation and the operation of the voluntary code of practice for RFID in New Zealand before deciding whether any further regulation is necessary. The Privacy Commissioner is well placed to monitor and assess these matters. For now, we think the Privacy Act and the voluntary code provide an adequate framework for regulating the use of RFID technology to collect and store personal information. If more specific, mandatory regulation is considered

152 See unit standards listed under "Domain – Electronic Security" on the NZQA website www.nzqa.govt.nz (accessed 11 December 2009).

153 See Cervin, above n 139, 76; "Public Space Surveillance (CCTV)" on the website of the Security Industry Authority (UK), www.the-sia.org.uk (accessed 11 December 2009).

154 *Privacy and CCTV*, above n 144, guideline 2.5.

155 Wellington City Council "New CCTV Cameras to Boost Central-City Safety" (14 April 2005) www.wellington.govt.nz (accessed 11 December 2009).

156 Privacy Stage 1 NZLC SP19, above n 134, 142-145.

157 GS1 New Zealand *EPC/RFID Consumer Protection Code of Practice* available at www.gs1nz.org.

158 Privacy Stage 3 issues paper, above n 135, 262-263.

necessary in future, one option would be to develop a code of practice for RFID under the Privacy Act. To the extent that RFID tags can be used to track people and objects, the tracking device offence that we recommend for inclusion in the Surveillance Devices Act will also help to control the improper use of RFID technology.

- 4.21 We also raised the issue of RFID skimming in our issues paper. Skimming is the covert use of RFID scanners to obtain information stored on RFID chips. We recommend in chapter 3 that RFID skimming should be considered as part of a broader review of the adequacy of New Zealand law to deal with data surveillance.

RECOMMENDATION

R19 Both Closed-Circuit Television (CCTV) and Radio-Frequency Identification (RFID) should be regulated within the Privacy Act framework, rather than under specific statutes or regulations. The Privacy Commissioner should continue to monitor the adequacy of existing law to deal with these technologies. If a more specific regulatory framework is considered necessary in future, the option of developing codes of practice under the Privacy Act should be considered.

RECOMMENDATION

R20 A code of ethics for private security personnel who install, advise on, operate and monitor CCTV systems should be made under the Private Investigators and Private Security Guards Act 1974 or any replacement statute. The code of ethics should address legal and ethical requirements in relation to privacy. Any prescribed training in relation to CCTV for private security personnel should also cover privacy obligations.

IMPROVING THE PRIVACY ACT'S COVERAGE OF SURVEILLANCE

- 4.22 In our issues paper we highlighted a number of ways in which the Privacy Act's application may be somewhat ambiguous or may be limited by the current wording of the Act.¹⁵⁹ There was a significant level of support from submitters for clarifying the Act's application to surveillance and closing any gaps in its coverage.
- 4.23 In our issues paper for stage 4 of this Review, we will be proposing the following changes to the Privacy Act, which we believe will improve its coverage of surveillance:
- The definition of "collect" should be amended so that it does not exclude the receipt of unsolicited information. It has been suggested that information obtained by the use of surveillance devices is not "solicited" from anyone, and therefore that such surveillance does not constitute collection under the Act as currently worded. While there are valid points to be made both for and against this interpretation, we think it should be put beyond doubt that surveillance is a form of collection of personal information.

¹⁵⁹ See particularly Privacy Stage 3 issues paper, above n 135, 55-58, 219-220.

- Privacy principle 3 should not refer to collecting personal information “directly” from the person concerned. Again, it has been suggested that where a surveillance device is used, the information is not collected “directly” from the person, and therefore the notification requirements under principle 3 may not apply.
 - Privacy principle 4 (which provides that information shall not be collected by means that are unlawful, unfair, or unreasonably intrusive upon the personal affairs of the individual) should be amended so that it applies to *attempts* to collect information. This would mean that principle 4 could be used to deal with situations in which an attempt is made to collect information using surveillance but no information is actually obtained. People who have been the focus of surveillance may feel that their privacy has been violated even when the attempt to collect information about them has been unsuccessful.
 - The scope of section 56 of the Act should be narrowed. Section 56 provides an exception to the privacy principles in respect of information collected or held by an individual solely or principally in connection with his or her personal, family or household affairs. This is a necessary exception, but a very broad one. As we illustrated in the surveillance scenarios which we set out in our issues paper, many instances of surveillance conducted by individuals might be covered by this exception. We will propose that, at a minimum, this exception should not apply where a person collects information by engaging in misleading conduct, or in an unlawful manner. We will also discuss some other options for narrowing the scope of section 56.
- 4.24 At present, the amendments set out above are proposals rather than recommendations. Because they have implications that go beyond surveillance, we will call in our issues paper for submissions on these proposals. The issues paper will also explain and develop these proposals further.

Chapter 5

Other remedies and penalties for intrusion

- 5.1 So far in this report we have discussed the need for a more comprehensive framework of criminal offences and matching civil remedies for invasion of privacy by surveillance, and have considered the Privacy Act's role in regulating surveillance. In our issues paper we also considered whether there were any other ways in which the law should provide better protection against intrusion and surveillance. One option, discussed in chapter 7, is a tort of invasion of privacy by intrusion into solitude, seclusion and private affairs. The issues paper also identified two other areas in which existing legal protections could be strengthened: harassment and voyeurism.¹⁶⁰ We discuss these two issues in this chapter.

THE HARASSMENT ACT 1997

- 5.2 In our issues paper we raised the question of whether surveillance activities might come within the ambit of the Harassment Act 1997. If so, the remedy of a restraining order would be available in appropriate circumstances. Section 3 of the Act provides that a person harasses another:

if he or she engages in a pattern of behaviour that is directed against that other person, being a pattern of behaviour that includes doing any specified act to the other person on at least 2 separate occasions within a period of 12 months.

- 5.3 "Specified act" is defined in the following way:

4 Meaning of specified act

(1) For the purposes of this Act, a specified act, in relation to a person, means any of the following acts:

- (a) Watching, loitering near, or preventing or hindering access to or from, that person's place of residence, business, employment, or any other place that the person frequents for any purpose:
- (b) Following, stopping, or accosting that person:
- (c) Entering, or interfering with, property in that person's possession:

¹⁶⁰ New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington, 2009) 239, 270-272 [Privacy Stage 3 issues paper].

- (d) Making contact with that person (whether by telephone, correspondence, or in any other way):
 - (e) Giving offensive material to that person, or leaving it where it will be found by, given to, or brought to the attention of, that person:
 - (f) Acting in any other way –
 - (i) That causes that person (**person A**) to fear for his or her safety; and
 - (ii) That would cause a reasonable person in person A's particular circumstances to fear for his or her safety.
- 5.4 Harassment is only criminal if the person engaging in the activity intends the other to fear for his or her safety or the safety of a family member or knows that the harassment is likely to cause such fear. However, a restraining order does not require any such element of intention. Section 16 of the Act provides as follows:

16 Power to make restraining order

- (1) Subject to section 17, the Court may make a restraining order if it is satisfied that –
 - (a) The respondent has harassed, or is harassing, the applicant; and
 - (b) The following requirements are met:
 - (i) The behaviour in respect of which the application is made causes the applicant distress, or threatens to cause the applicant distress; and
 - (ii) That behaviour would cause distress, or would threaten to cause distress, to a reasonable person in the applicant's particular circumstances; and
 - (iii) In all the circumstances, the degree of distress caused or threatened by that behaviour justifies the making of an order; and
 - (c) The making of an order is necessary to protect the applicant from further harassment.
 - (2) For the purposes of subsection (1)(a), a respondent who encourages another person to do a specified act to the applicant is regarded as having done that specified act personally.
 - (3) To avoid any doubt, an order may be made under subsection (1) where the need for protection arises from the risk of the respondent doing, or encouraging another person to do, a specified act of a different type from the specified act found to have occurred for the purposes of paragraph (a) of that subsection.
- 5.5 Section 17 provides a defence as follows:

17 Defence to prove that specified acts done for lawful purpose

A specified act cannot be relied on to establish harassment for the purposes of section 16(1)(a) if the respondent proves that the specified act was done for a lawful purpose.

Application to surveillance

- 5.6 The Harassment Act was originally passed in response to concerns about the activities of gangs and about stalking.¹⁶¹ There have been many cases on the Act since it came into force. Indeed, there is an average of 190 applications a year

¹⁶¹ The Explanatory Note to the Introduction copy of the Harassment and Criminal Associations Bill said: "The common theme underlying all parts of the Bill is that, although most measures are of general application, they are of particular significance in addressing concerns about gang behaviour." In Parliament, the then Minister of Justice, DAM Graham, characterised the harassment provisions of the Bill as dealing with the problem of stalking: (20 November 1997) 565 NZPD 5534.

for restraining orders.¹⁶² A case law website lists 73 judgments of the District Court and High Court relating to the Act.¹⁶³ Very few of the decided cases relate to gang activity. The Act is clearly of wide application. It has been described in the Court of Appeal as related to privacy. In the judgment of Gault P and Blanchard J in *Hosking v Runting*¹⁶⁴ it was one of the statutory provisions referred to as “recognising the privacy value and entitlement to protection”.

- 5.7 Some of the specified acts which can constitute harassment are already wide enough to encompass some forms of surveillance: “watching” in section 4(1)(a), “following” in section 4(1)(b), and “entering property” in section 4(1)(c). It seems to us that filming people’s activities, tracking their movements, or tapping their telephone calls can in certain circumstances amount to harassment as much as any of the activities which are expressly spelled out in section 4(1)(a)-(e). Those things are probably not covered at the moment. We think they should be. We believe that “keeping that person under surveillance” should be added to the list of specified acts in section 4(1). Equivalent provisions in the legislation of four Australian states specify keeping a person under surveillance as one of the acts which constitute stalking (although in all instances the Australian legislation creates a criminal offence).¹⁶⁵ One group which made submissions to us on the issues paper suggested that surveillance should only become harassment if it causes a person to fear for his or her safety. But we would prefer not to qualify the provision in this way. Fear for safety is not a requirement of paragraphs (a) – (e) of section 4(1).¹⁶⁶ The requirement for a restraining order that the behaviour must cause, or threaten to cause, the applicant distress is a sufficient qualifier. An intent to cause fear for safety would be relevant only to criminal liability.
- 5.8 However, if surveillance activity is to be a “specified act” a number of problems arise.
- 5.9 First, the Harassment Act provides expressly that to constitute surveillance there must be a “pattern of behaviour” which includes doing a specified act on at least two separate occasions over a twelve-month period. Thus, as it presently stands, a continuous single act of surveillance (for example, a camera trained on someone’s property) would not qualify even if it lasts for days or weeks. That is anomalous. Such continued activity can cause distress just as much as two short single instances within a twelve-month time frame. We therefore propose that the Harassment Act be amended to provide that, as well as repeated conduct, a single protracted instance should be enough to constitute harassment. There is precedent for this solution. Queensland has amended the stalking offence in its Criminal Code Act to provide that all that is required is conduct “engaged in on any 1 occasion if the conduct is protracted

162 Data for the years 2003/2004 – 2007/2008 supplied by the Ministry of Justice.

163 The Briefcase database, www.brookersonline.co.nz.

164 *Hosking v Runting* [2005] 1 NZLR 1, paras 106-108.

165 Crimes Act 1958 (Vic), s 21A; Criminal Law Consolidation Act 1935 (SA), s 19AA; Criminal Code Act 1924 (Tas), sch 1, s 192; Criminal Code Act 1983 (NT), sch 1, s 189. The Australian state legislation describes the activity as “stalking” rather than “harassment”, but the analogy with the New Zealand Act is close: the same kinds of conduct are covered. Because the Australian provisions create criminal offences, the intent to cause fear for safety is an element.

166 It is, however, of s 4(1)(f). See the judgment of Potter J in *Beadle v Allen* [2000] NZFLR 639, paras 36-40.

or on more than 1 occasion”.¹⁶⁷ We think it is unnecessary to prescribe a particular length of time. A restraining order can only be issued if the act is such as to cause distress, and that, it seems to us, is a sufficient criterion. It would be for the Court to determine whether the surveillance was in the particular case of such a kind, and of such duration, as to cause distress justifying the making of the order.

- 5.10 Nor is there any difficulty with the expression “pattern of behaviour” in section 3. A single protracted act can without artificiality be regarded as falling within the phrase “pattern of behaviour” for the purpose of that section. Section 21A of the Crimes Act 1958 (Victoria) (the “stalking” offence) which uses the similar phrase “course of conduct” in relation to stalking was interpreted in such a way by McDonald J. He said:¹⁶⁸

For example, a “course of conduct” which includes keeping the victim under surveillance, may comprise conduct which includes keeping the victim under surveillance for a single protracted period of time or on repeated separate occasions.

- 5.11 We therefore recommend that section 3 of the Harassment Act be amended to provide that a pattern of behaviour can be constituted *either* by doing a specified act on at least two separate occasions *or* by a single protracted act.
- 5.12 There is a further possible difficulty. It relates to the situation where the surveillance is covert, and is for some time unknown to the subject. We believe that in such a case the subject should be entitled to a remedy when he or she finally discovers the existence of the surveillance, provided he or she can produce sufficient evidence to satisfy the court that the surveillance is of a continuing nature. We do not believe any amendment is needed to the Act to achieve this result. In the United Kingdom case of *Howlett v Holding*,¹⁶⁹ Mrs Howlett had discovered she was under secret surveillance and was told that it would continue. The argument was presented to the Court that Mrs Howlett could not be harassed within the terms of the Protection from Harassment Act 1997 by surveillance of which at any given moment she was unaware. Eady J said:¹⁷⁰

This gives rise to a potentially very sinister scenario. One citizen is aware that another wishes to keep her and her home under surveillance ... It seems counter-intuitive that the court should be able to do nothing to allay her concerns ... What causes the distress is the awareness that secret surveillance is taking place, or is likely to take place at any moment.

- 5.13 A third difficulty relates to the defence of lawful purpose in section 17. As we have shown elsewhere in this report, surveillance is sometimes justified. That is most clearly so when it is carried out by law enforcement officers under warrant, but may also sometimes be true of, for example, the media, who may use a hidden camera to obtain information of real public concern where there is no other effective method of obtaining it. In such circumstances section 17,

167 Criminal Code Act 1899 (Qld), sch 1, s 359B(b). Emphasis added.

168 *Gunes v Pearson and Tunc v Pearson* (1996) 89 A Crim R 297, 306.

169 *Howlett v Holding* [2006] EWHC 41 (QB).

170 *Ibid*, paras 21 and 23.

the “lawful purpose” defence, may well be called in aid, and we think it would meet the case. However, it should not be thought that the defence of lawful purpose will justify even the most extreme forms of harassment, whether by surveillance or otherwise. The courts have interpreted this difficult section in a manner which requires that the activity must be proportionate to the purpose. In *Irvine v Edwards*,¹⁷¹ Judge Kerr, in a passage later approved by Potter J in the High Court,¹⁷² said:¹⁷³

I interpret section 17 to mean that if a respondent’s behaviour is lawful then on the face of it harassment does not occur, but it would seem to me that acts lawful in themselves may nonetheless support the making of a restraining order if the ways in which those acts are performed or undertaken creates harassment.

- 5.14 Indeed, in the High Court in *Beadle v Allen*, Potter J put it that in section 17 “Parliament gives the judge a *discretion* to refuse an order if the acts were done for a lawful purpose such as investigative journalism.”¹⁷⁴ The tenor of these remarks is that even if the purpose for which the activity is undertaken is lawful, the ends do not always justify the means. Conduct which goes further than necessary to fulfil the purpose may still be subject to a restraining order.
- 5.15 In the United Kingdom the courts have on a number of occasions used the harassment legislation to curb the activities of the paparazzi, although there the defence is expressed in a different, and perhaps more transparent, way: it requires that the conduct in question be “reasonable” in the circumstances.¹⁷⁵ In New Zealand, the Bill of Rights Act 1990 also needs to be factored into the exercise so that any restraining order must be a justified limitation on the rights and freedoms in the Bill of Rights.¹⁷⁶
- 5.16 It would be our preference that the lawful purpose defence should be reformulated to more clearly reflect the element of proportionality, but this is an issue which goes wider than the scope of this report.
- 5.17 The New Zealand Act, unlike the United Kingdom one, does not provide for a damages remedy. Such a provision is worth consideration, but again goes beyond the scope of this project. The Commission believes the Harassment Act merits separate review. The points raised in paragraphs 5.16 and 5.17 could be attended to in such a review.

RECOMMENDATION

R21 Section 4 of the Harassment Act 1997 should be amended by adding a new paragraph (ea): “Keeping that person under surveillance”.

171 *Irvine v Edwards* [1999] DCR 171. See also *Espinoza v Commissioner of Police* [1999] DCR 686, 690-691 Judge Morris.

172 *Beadle v Allen*, above n 166, para 27.

173 *Irvine v Edwards* [1999] DCR 171, 174.

174 *Beadle v Allen*, above n 166, para 50.

175 Protection from Harassment Act 1997 (UK), s 1(3)(c).

176 See *Beadle v Allen*, above n 166, paras 41-57; *B v Reardon* [2000] DCR 575, paras 22-25.

RECOMMENDATION

R22 Section 3 of the Harassment Act 1997 should be amended by providing that a pattern of behaviour can be constituted either by a single protracted act or by doing a specified act on at least two separate occasions within a period of 12 months.

VOYEURISM

5.18 Voyeurism can be defined as the observation (usually covert) for sexual gratification of persons in intimate situations such as the shower, toilet or bedroom. The term “peeping Tom” is often used of perpetrators. In its study paper *Intimate Covert Filming*,¹⁷⁷ the Law Commission set out the results of its research on voyeurism. It noted that some voyeuristic behaviour is symptomatic of a more serious and compulsive disorder. Research evidence links voyeurism with other more serious sexual offences. Apart from the implications for sexual offending, however, it is of particular relevance to our present project that voyeurism is one of the most extreme invasions of privacy. Reports of court cases involving it often refer to the distress of the victims:

- “When I saw the view someone was getting of us in our most personal moments I was outraged”.¹⁷⁸
- “The victims that were aware of the offending had been severely affected ... they worried about their children using public toilets and were unable to sleep at night.”¹⁷⁹

5.19 The question is whether New Zealand law sufficiently protects against such behaviour. There are several statutory provisions which can be called in aid. Section 30 of the Summary Offences Act 1981 provides:

30 Peeping or peering into dwellinghouse

- (1) Every person is liable to a fine not exceeding \$500 who is found by night without reasonable excuse –
- (a) peeping or peering into a dwellinghouse; or
 - (b) loitering on any land on which a dwellinghouse is situated.
- (2) In this section the term **night** means the period commencing on the expiration of the first hour after sunset and ending at the beginning of the last hour before sunrise.

5.20 It has been said that the offence does not require a “prurient motive”, but “it will often take place in that context.”¹⁸⁰ However, section 30 is limited to activity in relation to a *dwellinghouse*, to activity *outside* that dwellinghouse, and to activity *at night*. It is very narrowly focussed.

5.21 Section 29 of the Summary Offences Act 1981 is also relevant. Subsections (1) and (2) relevantly provide:

177 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) paras 2.34-2.39.

178 Theresa Garner “The Peeping Tom, the Judge and I...” (15 January 2000) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 22 December 2008).

179 Nick Churchouse “Peeping Tom Hid in Toilet” (29 Apr 2006) *Dominion Post* Wellington (accessed via Newztext database).

180 *Police v Pain* [1984] 2 NZLR 678, 679 Quilliam J.

29 Being found on property, etc, without reasonable excuse

- (1) Every person is liable to imprisonment for a term not exceeding 3 months or a fine not exceeding \$2,000 who is found without reasonable excuse –
- (a) in or on any building; or
 - (b) in any enclosed yard or other such area; or
 - (c) in or on board any aircraft, hovercraft, or ship or ferry or other vessel, train, or vehicle.
- (2) It is not necessary in a prosecution under this section for the prosecutor to prove that the defendant had an intention to commit any other offence, but it is a defence if the defendant satisfies the Court that he had no such intention.
- 5.22 This provision is not directly related to voyeurism, although it could be used to deal with some instances of it. But again it is limited. It deals essentially with trespassory conduct: conduct where the offender is on premises where he or she has no right to be. It would probably not be able to be used where a person was on public property (say in public toilets) or in his or her place of employment.
- 5.23 Section 11 of the Summary Offences Act 1981 may also be able to be called in aid on some occasions. If the accused damages property, for example by drilling holes to observe the conduct, he may commit the offence of wilful damage.
- 5.24 If the conduct in question took place in, or within view of, a public place, section 4(1)(a) of the Summary Offences Act 1981 might be appropriate to deal with a case of voyeurism. It provides:
- 4(1) Every person is liable to a fine not exceeding \$1,000 who, –
- (a) in or within view of any public place, behaves in an offensive or disorderly manner.
- 5.25 Case law establishes that offensive behaviour is conduct which is calculated to arouse anger or resentment or disgust or outrage in the mind of a reasonable person of the kind subjected to the behaviour.¹⁸¹ It is still an open question whether there is an additional requirement of risk to public order.¹⁸²
- 5.26 Sections 216G-216N of the Crimes Act 1961 render the covert filming of intimate activity an offence punishable by up to three years' imprisonment. These provisions protect the kinds of intimate activity to which we have referred, but are confined to "visual recording (for example a photograph, videotape, or digital image)". This includes a visual recording made and transmitted in real time, without retention or storage.¹⁸³ The intimate covert filming provisions do not, however, cover observation of intimate conduct without the use of a recording device.
- 5.27 In chapter 3 of this report we recommend a new offence of visual surveillance using a device. If this recommendation is adopted it would criminalise visual surveillance of activity in a dwelling which might include, but will not be limited to, intimate acts. But that recommendation is confined to the use of surveillance *devices*.

181 *R v Rowe* [2005] 2 NZLR 833 (CA), para 23; *Brooker v Police* [2007] 3 NZLR 91 (SC), para 55.

182 Compare *Brooker v Police* [2007] 3 NZLR 91 (SC), paras 31 and 118, and *R v Morse* [2009] NZCA 623, paras 26, 27 and 102-104.

183 Crimes Act 1961, s 216G(2).

5.28 It is clear that this collection of offences is patchy. Most of them do not specifically relate to voyeuristic behaviour at all. We take four instances which have been reported in New Zealand newspapers in recent years, and ask how they can be dealt with under the present law.

5.29 *A man was seen looking in the windows of two houses at about 6:30 am, “watching the residents inside getting ready for the day”. It is not clear from the report whether he was on the property, or looking from the street.*¹⁸⁴

The man would not be caught by section 30 of the Summary Offences Act, because in early April (which was when the incident occurred) 6:30 am would be later than an hour before sunrise – even though it is the very time when people would be likely to be getting dressed. If he was not in an “enclosed yard or other such area” he would escape section 29 as well. If he was on the street, section 4, the “offensive behaviour” provision, might have been able to be called in aid, but it is not entirely clear that his conduct could be characterised as “offensive”.

5.30 *A man was caught peering through two holes drilled in the bathroom floor of a house occupied by four young women. He would have had to grab wooden beams and haul himself into a “coffin-sized crawl space” and lie on his back to look through the holes.*¹⁸⁵

Section 30 of the Summary Offences Act would not apply unless this had occurred during the hours of darkness, which is unlikely. He could probably not be charged with being *in* a building for the purposes of section 29, although he probably could be charged with being in an enclosed yard. If it could be proved that he had drilled the holes in the floor he could be charged with wilful damage to property under section 11 of the Summary Offences Act 1981.

5.31 *A man broke into service panels behind a women’s public toilet, concealed himself there and made a small hole to peep through.*¹⁸⁶

He could have been charged with wilful damage. Even though this was a public toilet his activities were hidden, so the applicability of section 4 of the Summary Offences Act is unclear. He may possibly have been able to be charged under section 29 of the Summary Offences Act, even though this was a public toilet, because he was in part of the premises he was not entitled to enter.

5.32 *A woman in a public toilet discovered a man spying on her over the top of a cubicle.*¹⁸⁷

Probably the only provision under which he could be charged is section 4(1)(a) of the Summary Offences Act. The toilets were a public place, and his conduct could probably be characterised as offensive.

5.33 The legal responses to these situations are not very satisfactory. The person in the first example may not have been able to be charged with anything. In the case of the other three the Police would probably have been able to find

184 “Police Hunt Peeping Tom” (6 Apr 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 6 August 2009).

185 Garner, above n 178.

186 Churchouse, above n 179.

187 Ursula Hudson “Peeping Tom Lurking” (15 June 2005) *East and Bays Courier* Auckland (accessed via Newztext database).

provisions within which to bring the conduct, but none of those provisions is specifically aimed at the essence of the conduct to which objection is taken. The culprit could be successfully prosecuted only if he had committed some other offence. The present patchy collection of offences requires the Police to trawl through them to find the one which is the best “fit” for what has happened. The law can deal with the objectionable conduct, voyeurism, only indirectly.

- 5.34 The issue is finely balanced, but overall we think the law should be able to directly address behaviour of this kind.
- 5.35 Other jurisdictions have enacted provisions which directly make voyeurism an offence, even though it takes place without filming or recording, and without the use of any device. Thus, the Sexual Offences Act 2003 (UK) provides that a person commits an offence if “for the purpose of obtaining sexual gratification, he observes another person doing a private act”, knowing that the other person does not consent to being viewed in this way.¹⁸⁸ “Private act” is defined as an act carried out in a place which would reasonably be expected to provide privacy, and where the victim’s genitals, buttocks or breasts are exposed or covered only by underwear, or the victim is using a lavatory or is doing a sexual act that is not of a kind ordinarily done in public.¹⁸⁹
- 5.36 The Canadian Criminal Code provides that anyone commits an offence “who, surreptitiously, observes – including by mechanical or electronic means ... a person who is in circumstances that give rise to a reasonable expectation of privacy”.¹⁹⁰ As with the United Kingdom legislation, the provision goes on to define the kinds of intimate activity it is designed to cover.
- 5.37 The Crimes Act 1900 (NSW)¹⁹¹ and the Criminal Code Act 1899 (Qld)¹⁹² make similar provision. In each case, the offence is committed by merely *observing*. Filming or recording is not a necessary requirement.
- 5.38 The Law Commission believes that New Zealand should have similar legislation, and that this should be done by extending the intimate covert filming provisions, currently in the Crimes Act, to make it an offence to observe the type of intimate activity with which those provisions are already concerned. We thus recommend that it should be an offence to deliberately observe, without consent:
- a person who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and that person is—
- (i) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or
 - (ii) engaged in an intimate sexual activity; or
 - (iii) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing.

188 Sexual Offences Act 2003 (UK), s 67.

189 Ibid, s 68.

190 Criminal Code RSC 1985 c C-46, s 162.

191 Crimes Act 1900 (NSW), s 91J.

192 Criminal Code Act 1899 (Qld), sch 1, s 227A.

- 5.39 We have considered whether, if voyeurism is to be an offence, there is any need to retain the “peeping and peering” offence in section 30 of the Summary Offences Act 1981. We conclude that there is, to cover the case of the person who looks into a dwellinghouse window for the purpose of observing intimate activity, but who fails to see anything. There is, we think, a need to deter prowlers who make a practice of *attempting* to observe such activity. However, section 30 in its present form is manifestly unsatisfactory. The phrase “peeping and peering” is antiquated and unclear, and the restriction to night time is irrational. We thus recommend that section 30 be reformulated to make it an offence to look repeatedly or for a prolonged period into a dwellinghouse, without any limitation of the offence to night time. We consider that the current section 30(1)(b) (loitering on land on which a dwellinghouse is situated) is unnecessary as section 29 of the Act (being found on property) effectively covers the same conduct.
- 5.40 It is not our intention that the offence should catch persons looking into the window of a house in the course of perfectly legitimate conduct such as inspecting a home with a view to purchase. The question is how best to exclude such innocent conduct. One option would be to continue with the current formulation of “without reasonable excuse”, but that is undesirably vague. There is little doubt that the overwhelming rationale for the present section 30 is to deal with cases of prolonged looking with “prurient interest”, or sexual motive. Persons looking into a window for another nefarious purpose, such as planning a burglary, would be likely to enter the property and thus be caught by section 29. We think, therefore, that section 30 should be confined to persons acting for the purpose of sexual gratification. That may sometimes be difficult to prove, but will usually be indicated by the focus of the accused’s attention (bedroom or bathroom windows) and by the accused’s other conduct.

RECOMMENDATION

- R23 It should be an offence to deliberately observe without consent, whether with or without a device, for purposes of sexual gratification, conduct of the kind defined in the Crimes Act 1961, section 216G(1)(a).

RECOMMENDATION

- R24 Section 30 of the Summary Offences Act 1981 should be repealed and replaced with a provision that makes it an offence to look repeatedly or for a prolonged period into a dwellinghouse for the purpose of obtaining sexual gratification. The offence should not be limited to night time.

Chapter 6

Specific sectors

6.1 In our issues paper, we gave separate consideration to three sectors which raise particular challenges in terms of balancing privacy with other legitimate interests, and which are already governed by laws or regulatory mechanisms that are particular to each sector and that place some controls on surveillance. The three sectors were the media, the private investigation industry, and the workplace.¹⁹³ We now present our conclusions about issues specific to these three sectors.

THE MEDIA

- 6.2 We noted in our study paper for stage 1 of the Review the critical importance of a free media to a democratic society.¹⁹⁴ We learn almost all we know of events in our society through the media. This is no less true today than it was fifty years ago. Without the media we would live in what has been described as “an invisible environment”. The guarantee of freedom of expression in section 14 of the New Zealand Bill of Rights Act 1990 supports this essential media freedom.
- 6.3 However, times change, and recent times have witnessed increasing changes in our media environment.
- 6.4 First, there is an increasing merging of news and entertainment. The personal and the sensational attract readers, listeners and viewers.
- 6.5 Secondly, there is pressure to cut costs. Fewer staff and reduced resources mean increasing sameness of content in publications within the same ownership, and increasing resort to less expensive ways of getting stories, for example by using the internet as a source, and using material sent in by members of the public (citizen journalism).
- 6.6 Another development is the way in which the new technology has transformed methods of communication. On the one hand it has led to numerous new ways for ordinary citizens to convey information and opinions through blogs, chat rooms and sites like Facebook, Bebo and YouTube. On the other hand it

¹⁹³ New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington, 2009) ch 12 [Privacy Stage 3 issues paper].

¹⁹⁴ New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, Wellington, 2008) 196 [Privacy Stage 1 NZLC SP19].

has led to the phenomenon known as convergence, whereby publications which have traditionally been in one form of media now also make use of another. The review of the Press Council put it this way:¹⁹⁵

Examples were given of newspaper and television companies with websites that contain video clips, radio broadcast clips as well as the written word. Broadcasts of written work, movies, and real time picture news occur over the internet. Others pointed out that any one journalist may well, in the course of a day, present on live television, make a radio broadcast and produce copy for print publication. Thus, the activities of broadcast and print organisations and their professional employees indicate that the different forms of media are intertwined.

- 6.7 These developments provide challenges for any coherent definition of the term “news medium”; and also for the work of the media regulators which were set up on the basis of traditional media. Material on the internet is often substantially unedited and unsupervised. If it finds its way into mainstream media the risks of overstepping legal boundaries are obvious.
- 6.8 Given these developments, it is obvious that the media freedom of which we spoke must be limited by reasonable and justified provisions which protect privacy (among other things). As our issues paper demonstrated, such limitations exist in the form of the *Hosking* tort, various types of criminal liability, and the work of the regulators, the Press Council and the Broadcasting Standards Authority.
- 6.9 Yet, despite the risks to which we have adverted, invasion of privacy has not been a major part of the work of either the media regulators or the courts. Since the decision in *Hosking* in 2004 there appear to have been only four privacy tort cases before the courts.¹⁹⁶ In the 2008-2009 year, the Broadcasting Standards Authority determined 151 complaints, and a breach of the privacy standard was complained about in 17 (11 per cent) of these complaints.¹⁹⁷ In 2008 the Press Council determined only six complaints that were specifically concerned with privacy, out of a total of 43 complaints adjudicated (14 per cent).¹⁹⁸ Privacy featured well behind complaints about accuracy, fairness and balance, and lack of good taste. Nevertheless, despite the relatively low numbers, on occasion serious breaches of privacy do occur and there must be machinery to deal with them.

195 Ian Barker and Lewis Evans *Review of the New Zealand Press Council* (New Zealand Press Council, Wellington, 2007) 14.

196 These cases are referred to at para 7.3 below, and the three reported cases are discussed in more detail in Privacy Stage 3 issues paper, above n 193, 25-30.

197 Broadcasting Standards Authority *Annual Report 2009* (Wellington, 2009) 34.

198 New Zealand Press Council *36th Report of the New Zealand Press Council* (Wellington, 2008) 14, 29.

Regulatory controls

- 6.10 There are four points to be made in relation to media regulation.
- 6.11 The first relates to the matter of convergence. The Broadcasting Standards Authority deals with broadcasting as defined in the Broadcasting Act.¹⁹⁹ The Press Council deals with the print media, that is to say newspapers and magazines. Other forms of publications such as books, and in particular the internet, do not have dedicated regulators at all. They can be dealt with, if at all, only by complaint to the Privacy Commissioner. Information privacy principle 11 in the Privacy Act 1993, which prohibits unauthorised disclosure of personal information, is certainly in its terms wide enough to cover such forms of dissemination. The terms of that principle, and the procedures followed by the Privacy Commissioner, differ from those of the other regulators. Initially the Privacy Commissioner attempts resolution by techniques such as mediation, but if that fails the Human Rights Review Tribunal has jurisdiction to hear the case and can award damages. Principle 11 contains no “highly offensive” requirement (in contrast to the BSA privacy principles, which do include such a requirement). Nor is there any “public concern” defence as such, although some of the exceptions in principle 11 do go some of the way in that direction.²⁰⁰
- 6.12 There is a question whether any form of internet publication can lay claim to be a “news medium” and thus fall outside the Privacy Commissioner’s jurisdiction.²⁰¹ It is certainly possible to argue that an online newspaper, and possibly even some blog sites, might do so. If that is so, those publications would fall outside the jurisdiction of any of the regulators: the Privacy Commissioner because they are “news media”, the Broadcasting Standards Authority because they are not “broadcasting” and the Press Council because it does not deal with all online publications. We wonder whether there may be merit in amending the definition of “news medium” in the Privacy Act to resolve this dilemma, perhaps by providing that online publications which are not subject to any other regulator are not “news media” and thus are subject to the Privacy Commissioner’s jurisdiction. We defer full consideration to our review of the Privacy Act in stage 4 of this Review, and will call for submissions on this suggestion.
- 6.13 Another issue is that the media regulators perform their tasks in very different ways. There has been much comment that it is difficult to understand why broadcasters and the print media are dealt with so differently, the one by a statutory body which can impose legal sanctions, and the other by a voluntary body which cannot. However, New Zealand is not alone in this; it is the same across most of the world and we would need a very good reason for the New Zealand newspaper industry to be treated differently and more severely than its overseas counterparts, particularly when one considers that its track record in privacy matters is rather better than those of some overseas newspaper industries. The recent review of the New Zealand Press Council did not recommend any power to impose monetary sanctions, although it did recommend that there be a new power to censure in serious cases.

199 Broadcasting Act 1989, s 2(1).

200 For example principle 11(e) and (f).

201 Privacy Act 1993, s 2(1), definition of “agency” (xiii).

- 6.14 We also note the different principles operated by the Broadcasting Standards Authority and the Press Council. The Press Council Code is brief and general.²⁰² The Broadcasting Standards Authority Privacy Principles go into much greater detail and thus give greater guidance.²⁰³ Some overseas codes, particularly broadcasting codes, are even more detailed than this: the privacy section in the Ofcom code in the United Kingdom, for instance, is eight pages long. The recent Press Council Review recommended that attention be given to revising the Press Council principles.²⁰⁴ As far as privacy is concerned we agree with that recommendation, and hope that the privacy principle in particular can be spelt out in more detail.
- 6.15 There is, of course, a much wider issue which goes well beyond privacy, and is therefore beyond our present terms of reference. It is how, if at all, the internet can be regulated. The issue is vast and international, and does not appear close to a solution. Any jurisdiction the Privacy Commissioner may have over internet publication can of course deal only with privacy matters, a small part of the problem. The New Zealand Press Council Review says:²⁰⁵

The ease of entry, exit and re-location suggest that it will be difficult for New Zealand to enforce professional standards and norms – such as the respect of privacy; and for a New Zealand regulatory body – whether Government or industry – to obtain commitment to any regulatory regime from all those disseminating material in the internet.

It goes on to note that “the future is very uncertain in this area.”

- 6.16 A final, and quite specific, point concerns the BSA’s ability to award damages for breaches of privacy standards. The Broadcasting Act 1989 provides that, where the BSA finds that a broadcaster has failed to maintain standards that are consistent with the privacy of an individual, the Authority may order the broadcaster to pay up to \$5000 as compensation to that individual.²⁰⁶ The BSA cannot award compensation for breaches of any of the other standards. The amount that the BSA can award has not been increased since 1989, and seems low compared to the amounts that can be awarded for privacy breaches by the Human Rights Review Tribunal and the courts; it might well merit review. On the other hand, the Press Council is unable to award any compensation at all for privacy breaches in the print media.

Civil and criminal liability: media exemptions and defences

- 6.17 There is an important question of how far the media should be exempt from, or have a defence to, the general laws of the land when they are acting in the course of their news-gathering and dissemination activities. This is not a simple question.

202 See the Press Council Statement of Principles, principle 3.

203 The BSA principles can be found at <http://www.bsa.govt.nz/codesstandards-privacy.php>.

204 Barker and Evans, above n 195, 5 (rec II.3(m)), 72-73.

205 Ibid, 15.

206 Broadcasting Act 1989, s 13(1)(d).

- 6.18 Some criminal offences involve conduct so clearly against the public interest that it could not for a moment be supposed that the media should be exempt, however worthy their motives might be. Breaking and entering a private dwelling house, intimate covert filming, and demanding with menaces are examples so obvious that they go without saying.
- 6.19 In the case of other offences, however, an argument can be made that there should be an exemption for at least some types of media activity. The provisions of the Harassment Act 1997 are an example: it may at times be justifiable for the media to telephone a person or accost a person in the street on more than one occasion if information of legitimate public concern is being sought. Likewise, the Broadcasting Standards Authority allows a public interest exception to its intrusion principle,²⁰⁷ and on occasion has found hidden filming justifiable.²⁰⁸
- 6.20 In relation to other legal areas, there are real doubts. Can the media ever be justified, for example, in committing what would otherwise be a trespass on private land for the purpose of taking photographs? Most would say not. The ancient principle that a person's home is their castle would generally be thought to prevail. Even the Police need a warrant to enter private property.²⁰⁹
- 6.21 It is not possible to lay down any firm principles. Each statutory provision creating an offence, and every civil cause of action, must be examined on its merits. It is necessary to examine the interest protected by the law in question and to balance against it the interest protected by allowing limited exemptions from, and defences to, the offence. Bill of Rights Act considerations also need to be taken into account.
- 6.22 Supposing it is decided that there should be a media exemption or defence, the next question is how that exemption or defence should be framed. Should it be specific to the media, or should the net be cast more widely? There already exist some defences and exemptions which are quite specifically confined to the media. The Privacy Act itself is an example. Beyond the privacy area, there is a specific media exemption in the Fair Trading Act,²¹⁰ and a number of Acts regulating court proceedings give specific privileges to the media to remain in court when other members of the public have been excluded.²¹¹ Yet other Acts confer particular privileges on "journalists".²¹²

207 BSA Privacy Principles, above n 203, principle 8.

208 See *de Hart v TV3* (10 August 2000) Broadcasting Standards Authority 2000-108, and the discussion in Steven Price *Media Minefield: A Journalists' Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 70-72.

209 The current law achieves a compromise: it is not an offence to be found on land if there is reasonable excuse for being there (Summary Offences Act 1981, s 29) but if the person does not leave after a warning an offence is committed under section 3 of the Trespass Act 1980.

210 Fair Trading Act 1986, s 15.

211 See New Zealand Law Commission *Suppressing Names and Evidence* (NZLC R109, Wellington, 2009) 45 (n 69).

212 Evidence Act 2006, s 68; Financial Advisers Act 2009, s 12(a); Securities Markets Act 1988, s 2(1), definition of "investment advice".

- 6.23 On the whole, however, we believe that it is desirable to frame exemptions and defences in more general terms, particularly where the criminal law is concerned. For one thing, as we have seen, it is increasingly hard these days to define the media. It is no longer the preserve of the traditional broadcasters and print media. There may possibly be situations where the new media, including internet publication, also deserve special consideration. But, more importantly, it may be that a defence for the media should also be able to be shared by the authors and publishers of books; by researchers; and by citizens who pass information on to the media while not being members of the media themselves (citizen journalists).
- 6.24 We therefore prefer broader defences like the *Hosking* “legitimate public concern” defence, which protects the media along with other potential defendants who publish material with justified cause.
- 6.25 Currently there are defences which are much broader even than this. New Zealand law is well used to defences like “for a lawful purpose” (as in the Harassment Act 1997) and “reasonable excuse” (as in the Summary Offences Act 1981).²¹³ A surprising number of New Zealand statutes contain these phrases. The courts are used to handling them, and they do enable a balancing exercise involving the weighing of Bill of Rights considerations in each case. The media may sometimes be able to claim the benefit of them. As against this, they do not provide much clear guidance for those who must try in advance to assess whether the conduct they are contemplating will be in breach of the law. The ideal balance between flexibility and certainty can be very difficult to achieve.
- 6.26 In this report we have had to bear these considerations in mind when making our recommendations. We have opted to leave the *Hosking* tort where it is, with its “legitimate public concern” defence providing what we believe is appropriate protection for the media. Likewise, our recommendation that the Harassment Act 1997 be extended to cover surveillance is balanced by a “lawful purpose” exception. As for the new surveillance device offences we are recommending, we have deliberately kept them narrow, and targeted only truly objectionable conduct. We believe the defences to such offences should also be narrow. Thus, for example, the only defences we recommend to the proposed offence of visual surveillance of the interior of a dwelling (apart from law enforcement exceptions) are that the dwelling was at the material time being used as a place of work or business, or that the surveillance is believed to be necessary to protect health and safety or to bring to light the commission of an offence. The media will be able to rely on these defences. However, we have difficulty seeing that trespass to install a surveillance device can ever be justifiable except by law enforcement or intelligence agencies acting under warrant or other authorisation.

213 Harassment Act 1997, s 17; Summary Offences Act 1981, s 29.

Māori, privacy and the media

- 6.27 In the study paper for stage 1 of this Review, we included a preliminary discussion of Māori and privacy.²¹⁴ Since then, we have consulted a group of Māori from a range of backgrounds about privacy issues that affect Māori. Most of these issues relate primarily to the Privacy Act, and will be discussed in our issues paper for stage 4 of the Review. We will restrict our discussion in this report to issues concerning privacy and the media as they affect Māori.
- 6.28 Participants in our consultation meeting expressed concerns about media portrayal of Māori that went well beyond privacy. This is consistent with BSA research which suggests that:²¹⁵

While concerns about privacy remain an issue for some Māori, ... these take a back seat to the greater concerns about the mainstream media's representation or portrayal of Māori and its treatment of issues relating to Māori society...

There was, however, a feeling among those we talked to that Māori feel particularly watched and scrutinised as a result of the ways in which Māori individuals and communities come under the media spotlight. This has implications for the ability of Māori to protect their individual and collective privacy.

- 6.29 There are also cultural factors that may give rise to distinctive privacy concerns for Māori. One example is that many Māori may see the deceased as having some privacy rights, whereas complaints under both the Privacy Act and the Broadcasting Act can only be made in relation to living persons. The BSA reports that “[i]n only a few complaints has tikanga been central to the complaint”, but also that privacy (and particularly privacy of the deceased) is one area in which there has been conflict between Māori cultural standards and official broadcasting standards.²¹⁶ The BSA has carried out valuable research on Māori attitudes to privacy,²¹⁷ and there are now useful guides to Māori cultural protocols for journalists and film-makers working in Māori contexts.²¹⁸ Increased understanding of tikanga on the part of media representatives would assist them to better anticipate and handle Māori privacy concerns. As Māori Television submitted to us, this is not a matter that can be addressed by the law or by rigid rules:²¹⁹

[T]he question of how to deal with Māori issues relating to privacy in broadcasting comes down to a matter of how tikanga is implemented.... [T]he only way to move forward on the issue of privacy for Māori, is instead of trying to regulate via statute,

214 Privacy Stage 1 NZLC SP19, above n 194, 104-108.

215 Broadcasting Standards Authority *Maori Worldviews and Broadcasting Standards: What Should be the Relationship?* (Wellington, 2009) 20.

216 Ibid, 18-21 (quote at 18).

217 Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (BSA/Dunmore Press, Wellington, 2004) 56-60, and ch 4 for a national survey of attitudes that included a representative sample of Māori.

218 Carol Archie *Pou Kōrero: A Journalists' Guide to Māori and Current Affairs* (New Zealand Journalists Training Organisation, Wellington, 2007); Bradford Haami *Urutahi Koataata Māori: Working with Māori in Film and Television* (2 ed, Ngā Aho Whakaari, Auckland, 2008).

219 Māori Television, submission to the Law Commission, 11 May 2009.

or via common law, ... to look at pragmatically achieving an outcome or outcomes that are beneficial to all parties in a dispute regarding privacy issues. Doing the right thing does not necessarily mean applying strict principle to one case as it was applied in another.

The development by media organisations of protocols for recording in Māori communities and reporting on matters concerning Māori could help to improve media responsiveness to Māori concerns.

- 6.30 One specific issue concerns filming on marae. Generally speaking, permission is required for filming on marae, and sensitivity and discretion in filming or photographing are important. As Carol Archie advises journalists: “You are operating in an environment where tikanga Māori sets the rules and the marae is not a public place.”²²⁰ In chapter 3, we have suggested that buildings on a marae should be covered by the definition of “dwelling” for the purposes of the new offence of visual surveillance of a dwelling. This is partly because people carry out activities such as sleeping and bathing, which are characteristically performed in a dwelling, on marae. But perhaps more importantly, marae are homes in a spiritual and emotional sense for the whānau, hapū and iwi who affiliate to them. The offence only covers visual surveillance of the interior of buildings, so would not include the open areas within the marae boundaries. We recognise that matters of wider public interest are often discussed on marae, but we do not think that this gives people who do not belong to the marae a right to film inside its buildings without consent.

PRIVATE INVESTIGATORS

- 6.31 In the past, matrimonial matters formed a large part of the business of private investigators, particularly when adultery was still a ground for divorce. Today, while matrimonial and family matters can still form part of their work, private investigators deal with a much wider range of matters, including insurance fraud and claims investigation, missing persons investigations, corporate fraud and risk management, witness location, intellectual property protection and consumer investigation. They are sometimes used by government agencies and Crown entities. They perform much useful work.
- 6.32 Yet it is of the nature of their business that private investigators do some of their work undercover. Some of it effectively involves spying on people. If the industry were not regulated there would be substantial scope for abuse. As it is, several high-profile incidents involving private investigators in recent years have caused public unease and been the subject of much publicity. Currently, private investigators are regulated by the Private Investigators and Security Guards Act 1974, which creates a scheme of licensing of private investigators, and approval of their employees. The Registrar has disciplinary powers, including cancellation of licence. A Bill strengthening those regulatory controls is currently before Parliament.²²¹
- 6.33 Section 52 of the present Act imposes a substantial restriction on private investigators, its purpose being the protection of privacy. It provides as follows:

²²⁰ Archie, above n 218, 24.

²²¹ Private Security Personnel and Private Investigators Bill 2008, no 297-1.

52 Private investigator not to take photographs or make recordings without consent –

(1) Every person who, in the course of or in connection with the business of a private investigator,—

- (a) Takes or causes to be taken, or uses or accepts for use, any photograph, cinematographic picture, or videotape recording of another person; or
- (b) By any mechanical device records or causes to be recorded the voice or speech of another person,—

without the prior consent in writing of that other person, commits an offence against this Act:

Provided that nothing in this subsection shall apply to the taking or using by any person of any photograph for the purposes of identifying any other person on whom any legal process is to be or has been served.

(2) No photograph or cinematographic film, or videotape recording taken, or other recording made, in contravention of subsection (1) of this section shall be admissible as evidence in any civil proceedings.

6.34 A substantially similar provision appears in the new Bill (clause 66), although the penalty for infringement has been increased. When the Bill which led to the present Act was passing through Parliament, the then Minister of Justice explained that this provision was part of a suite of privacy protections which the Government intended to put in place.²²² Others included restrictions on the use of listening devices, and a statutory tort of invasion of privacy.

6.35 Section 52 is restrictive and has been a source of dissatisfaction in the industry for many years. It bans:

- photographing a person in any place, even a public place;
- arranging for someone else to take such photographs;
- “accepting” a photograph of someone with the purpose of using it; and
- the recording of any conversation, whether or not the private investigator is a party to the conversation, unless the other party agrees.

The part of the provision that deals with voice recording sits uneasily with the Crimes Act prohibition on the use of listening devices enacted in 1979.²²³

6.36 Thus, private investigators have fewer rights than other members of the public in this regard.

6.37 There are other illogicalities about the current provisions. They are old and have not kept up with the times; for example, it is only the use of mechanical audio recording devices which is prohibited, not electronic or digital devices, and there is no ban on the use of tracking devices.

6.38 Moreover, there are ways around some of the prohibitions in the current section 52. For example, security guards (as distinct from private investigators) are not prohibited from engaging in the activities which are

²²² Hon Dr AM Finlay (1 March 1974) 389 NZPD 564-565; (30 July 1974) 392 NZPD 3300-3301.

²²³ Now updated to cover all interception devices: Crimes Act 1961, ss 216A-216F.

covered by section 52, and may sometimes be able to be used to undertake them. Moreover, there is nothing to stop a private investigator from lending cameras to clients who can then take pictures for themselves.

- 6.39 The position is obviously unsatisfactory. Given the nature of private investigators' work there is no doubt that the industry needs to be regulated. But the better way to do so is by effective licensing and disciplinary procedures, rather than by artificially restricting the means by which they may acquire information. We believe that private investigators should have the same rights and duties in respect of filming, recording and obtaining information as any other member of the community. Those rights should be subject to the same limitations as apply to others, and the duties should be subject to the same defences. This was the view taken by the majority of submitters to answer this question in the issues paper. So, we recommend the repeal of section 52 and the deletion of its equivalent in the Bill currently before Parliament. However, it would be unsatisfactory to leave it at that as things currently stand because, as we have demonstrated, the general law on surveillance and invasion of privacy is piecemeal and unsatisfactory. For that reason, our recommendation of repeal is conditional on two further matters.
- 6.40 First, this report recommends that the general law on surveillance be reformed so that it provides effective and coherent protection for privacy. Chapters 2 to 5 deal with these matters. We recommend that the repeal of section 52 be contingent on the implementation of two of the general reforms we recommended in the earlier chapters:
- the enactment of a Surveillance Devices Act as recommended in chapter 3; and
 - the reforms to the Harassment Act recommended in chapter 5.

Should this not happen, section 52 will need to be revisited separately to bring it into line with modern needs.

- 6.41 Secondly, many industries whose activities impact on the public have codes of ethics. Broadcasters in New Zealand have a statutory code, newspapers a voluntary one. Public relations practitioners have a voluntary code based on international practice. In overseas jurisdictions, codes for the private investigation industry are very common. The Private Investigators and Security Guards Act 1974 provides for the making of regulations prescribing codes of ethics for private investigators and security guards.²²⁴ The Bill currently before Parliament contains a similar empowering provision for codes of *conduct*.²²⁵ This regulation-making power has never been exercised, nor has the industry developed a detailed voluntary code, although the New Zealand Institute of Professional Investigators (NZIPI) has a very brief code of ethics that applies to its members. We believe that a binding code would be a major step forward. There was support for it in submissions on the issues paper. Members of the industry themselves supported such a development. Such a code would provide a clear basis for the exercise of the disciplinary jurisdiction. We therefore believe that regulations should be made under the Act

²²⁴ Private Investigators and Security Guards Act 1974, s 71(h).

²²⁵ Private Security Personnel and Private Investigators Bill 2008, no 297-1, cl 106(1)(l).

for a code of ethics for private investigators, and that the repeal of the present section 52 should once again be conditional on that happening. To leave the matter to the industry to develop its own voluntary code would be less satisfactory because such arrangements can only bind persons who are members of the industry body, a point noted by the NZIPI in its submission.

- 6.42 We believe that the current legislation and the new Bill should be amended in one further respect. This relates to regulation of the industry rather than section 52. Under the Bill it is to be a ground for disqualification of an individual applicant for a licence that the individual has been convicted of various kinds of offence.²²⁶ They include a “specified offence” under the Criminal Records (Clean Slate) Act 2004 (these being sexual offences); offences of dishonesty and drug dealing; and an offence of working while unlicensed. We believe that there should be added to this list of disqualifying offences ones which involve serious invasions of privacy, in particular the intimate covert filming offence already contained in the Crimes Act, and the new surveillance offences we recommend in this report.²²⁷ There was general support for such a suggestion in submissions on the issues paper.

RECOMMENDATION

- R25 Section 52 of the Private Investigators and Security Guards Act 1974 should be repealed and the corresponding clause of the Private Security Personnel and Private Investigators Bill should be deleted. However, these changes should only be made after the following recommendations have been implemented:
- the enactment of a Surveillance Devices Act, as recommended in chapter 3;
 - the amendment of the Harassment Act 1997, as recommended in chapter 5; and
 - the introduction of a code of ethics for private investigators, as recommended in R26 below.

RECOMMENDATION

- R26 A code of ethics or code of conduct for private investigators should be made under the Private Investigators and Security Guards Act, or under the Private Security Personnel and Private Investigators Bill if that Bill is enacted. The code should address issues of privacy and the use of surveillance by private investigators.

²²⁶ Ibid, no 297-1, cl 41.

²²⁷ The offences in the Crimes Act relating to unlawful interception of private communications are already included in the list of disqualifying offences in the Private Investigators and Security Guards Act and the Private Security Personnel and Private Investigators Bill.

RECOMMENDATION

R27 Additional offences involving serious invasions of privacy should be added to the lists of disqualifying offences for private investigators and their employees in the Private Investigators and Security Guards Act or the Private Security Personnel and Private Investigators Bill. These offences should include the existing intimate covert filming offences, and the new surveillance device offences that we recommend in this report.

THE
WORKPLACE

- 6.43 As discussed in the issues paper,²²⁸ surveillance in the workplace can potentially take a number of forms, such as the use of cameras, the audio recording of telephone conversations, the installation of tracking devices in vehicles, and computer monitoring. In privacy terms, the workplace has points of difference from other contexts. On the one hand, employers have an interest in detecting theft or misconduct by employees, monitoring productivity, and keeping abreast of health and safety issues. Moreover workplaces, while often not public in the sense of being open to entry by the general public, are not private in the same way as is a person's home: employees can be observed by their co-workers and often by visitors as well. On the other hand, there are strong counter-arguments in favour of workers' privacy. The issues paper summarised them in this way:²²⁹
- The employment relationship is not an entirely voluntary one, and there are inequalities of power between employers and employees. Therefore, employees cannot be assumed to have freely consented to restrictions on their privacy, and workers need some legal protection of their privacy in order to redress the power imbalance.
 - Employers' property rights must be balanced against workers' fundamental human right to be treated with dignity and respect.
- 6.44 The workplace is of course governed by the general law. That includes the Privacy Act. The Privacy Commissioner may receive complaints from employees in the same way as from any other category of person. There are cases where the Commissioner has formed the opinion that an employer's actions were in breach of the Act.²³⁰ Quite apart from the complaints jurisdiction, the very existence of the Privacy Act 1993 serves to influence employer behaviour.
- 6.45 New Zealand employment law also assists in drawing a fair balance between the rights of employers and employees. In particular, the duty of good faith contained in the Employment Relations Act 2000 requires the parties to an employment relationship "to be active and constructive in establishing and maintaining a productive employment relationship in which the parties are, among other things, responsive and communicative."²³¹ The question is whether, in the light of the existing law, there is a need to make special provision for workplace surveillance. In the issues paper we asked for views on whether there

228 Privacy Stage 3 issues paper, above n 193, paras 12.24-12.39.

229 Ibid, para 12.31.

230 Ibid, para 12.34.

231 Employment Relations Act 2000, s 4(1A)(b).

should be a special Workplace Surveillance Act as exists in New South Wales, or whether a code of practice should be developed under either Section 46 of the Privacy Act 1993 or Section 100A of the Employment Relations Act 2000.

- 6.46 Those who made submissions acknowledged that the workplace raises special issues of the kind we mentioned above. However, this did not translate into a belief that change was required in the law. One submitter even suggested that any attempt to regulate workplace surveillance by law could actually undermine the trust, confidence and good faith upon which employment relations are built.
- 6.47 There was very little support for a separate workplace surveillance statute: only one submitter went that far. As for a code of practice, none of the employer organisations which made submissions were in favour. There was some support for a code from other quarters, but it could not be described as strong.
- 6.48 We have come to the view that the existing law is currently adequate to deal with workplace surveillance issues. Nor, as we have just indicated, can we point to any strong demand for a law change, or increased regulation. However, we believe that this matter should be kept under review by the Privacy Commissioner. If, in the light of future developments in technology or employment practices, the current privacy protection becomes inadequate, consideration should then be given to putting further controls in place. We would favour a code in the first instance, with a separate statute as a fall-back option if other forms of regulation fail.

Chapter 7

Tort of invasion of privacy

7.1 As we explained in the issues paper,²³² the New Zealand Court of Appeal in *Hosking v Runting*²³³ decided by a majority of three to two that there is a common law tort of invasion of privacy in New Zealand. Its ingredients, as formulated by Gault P and Blanchard J, are as follows:²³⁴

- (i) The existence of facts in respect of which there is a reasonable expectation of privacy; and
- (ii) Publicity given to those private facts that would be considered highly offensive to an objective reasonable person.

They also said there is “a defence enabling publication to be justified by a legitimate public concern in the information.”²³⁵ Their Honours said that the remedies available are damages and injunction.

7.2 The existence of such a tort had been foreshadowed and supported in High Court cases dating back 20 years. *Hosking* gave it authoritative recognition and formulation, even though by the barest of majorities. Two of the judges, Keith and Anderson JJ, dissented very strongly.

7.3 Since 2004 there have been three reported cases on the tort.²³⁶ In *Rogers v Television New Zealand Ltd*,²³⁷ three judges of the Supreme Court thought there could be no reasonable expectation of privacy in a murder confession made to Police, even though that confession was excluded from evidence at the trial. Anderson J continued to doubt whether there should be such a tort at all; Elias CJ believed that its elements, as stated in *Hosking*, might need further

232 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington, 2009) 21-26 [Privacy Stage 3 issues paper].

233 *Hosking v Runting* [2005] 1 NZLR 1 (CA).

234 *Ibid*, para 117.

235 *Ibid*, para 129.

236 It appears that, in addition to these three reported cases, there has been at least one other where an injunction was granted, but where publication of the details was suppressed: “Veitch’s Ex Seeks Ban on ‘Private Material’” (24 July 2009) *Dominion Post* Wellington www.stuff.co.nz (accessed 24 July 2009).

237 *Rogers v Television New Zealand Ltd* [2008] 2 NZLR 78 (SC).

refinement at some future time. *Andrews v Television New Zealand Ltd*²³⁸ clarified that there can sometimes be expectations of privacy in a public place and demonstrated how, even if there is a reasonable expectation of privacy, the plaintiff will still fail if the publicity is not highly offensive. *Brown v Attorney-General*²³⁹ demonstrated the difficulties which can sometimes arise in applying the “highly offensive” requirement and the public concern defence.

7.4 We noted in the issues paper some of the difficulties with the new tort.²⁴⁰ The major criteria are open-ended and involve the exercise of judgement which may sometimes be subjective. Given the early stages of development of the tort there are many gaps. It still remains to be decided, for instance, whether there are other defences than public concern, and other remedies than injunction and damages; whether the tort protects corporations as well as natural persons and the dead as well as the living; in exactly what situations there can be an expectation of privacy in a public place; and whether the tort can give a remedy for information which is false as well as information which is true. We noted that, given the paucity of litigation, development at common law would proceed slowly. In the issues paper we asked questions about the tort, the need for it, and its future development. We were assisted by the submissions we received.

7.5 We also asked in the issues paper a series of questions about areas of uncertainty in relation to the elements of the tort, and about gaps in the tort as it has developed so far through the common law. We asked these questions because, if we were to recommend that the tort be put on a statutory basis, we would need to make recommendations about the content of the statute. For reasons set out below, we have decided to recommend that the tort should be left to develop at common law. However, we received some very useful responses to our questions on the content of the tort, and we feel that there is value in making these views more widely available. We have therefore summarised in Appendix B the submissions we received on our questions about the content of the tort.

DO WE NEED THE TORT AT ALL?

7.6 Given the strength of the dissents in the Court of Appeal and Anderson J’s doubts in the Supreme Court we felt we needed to ask whether New Zealand should have such a tort at all. The great majority of submitters supported its retention. We agree with that view. For the legislature to abolish a tort which has only recently been introduced into the law after careful deliberation in one of our highest courts would require very good reason. No convincing reason has been provided to us. Submitters pointed out that the dignitary interest which privacy protects is important, and concerns about it are likely to increase rather than decrease over the years, given the march of new technology. The tort is a demonstration that the law treats the matter seriously. In applying it the courts have at their disposal a remedy, the injunction, which is available to no other

238 *Andrews v Television New Zealand Ltd* [2009] 1 NZLR 220 (HC).

239 *Brown v Attorney-General* [2006] DCR 630.

240 Privacy Stage 3 issues paper, above n 232, ch 6.

tribunal, and in appropriate cases they can award damages at a higher level than anyone else. In other words they can deal with very serious intrusions appropriately.

- 7.7 Moreover, to abolish the tort would be to go against international trends. There is a privacy tort, or something equivalent to it, in Europe and the United Kingdom, some provinces in Canada and the United States.²⁴¹ Both the Australian Law Reform Commission and the New South Wales Law Reform Commission have recommended a statutory cause of action in privacy. For us to abandon the tort would give an unfortunate signal to the international community about New Zealand's commitment to the protection of privacy. Nor can it be said that the existence of the tort threatens freedom of expression in New Zealand. Since the *Hosking* case was decided in 2004 only four cases of any significance have come before the courts, and two of them were decided in favour of the defendant. In addition, there is a specific defence for publication of information which is legitimately of public concern.

SHOULD THE
TORT BE
CODIFIED?

- 7.8 In the issues paper we noted the many gaps and uncertainties in the existing tort, and asked whether it should be enacted in statutory form. A statute would render the law more accessible than the common law (an advantage in itself), fill some of the gaps in the current law, and render some of the criteria more certain than they currently are. The common law is dependent on the accidents of litigation and develops slowly. Statute law can present a complete and coherent whole straight away.²⁴²
- 7.9 However, after careful deliberation we have decided that the tort should be left to develop at common law. The common law has the great advantage that in a fast-moving area judges can make informed decisions on actual cases as they arise. Privacy is particularly fact-specific. As has been said in the United Kingdom, each case requires an intense focus on the individual circumstances. The common law is well-suited to that task. The common law is also flexible, and can thus develop with the times. Statute creates a risk that what is enacted today may be out of date tomorrow. To avoid this dilemma, any privacy statute would have to be drafted in open-ended terms, and might end up being little advance on the common law.
- 7.10 Nor is there any evidence that the current state of the law is causing practical difficulties to anyone. We had wondered whether the media might want greater certainty than the law currently gives them. But our consultations with representatives of the media reassured us that they are comfortable with the broad and general direction the common law currently provides.
- 7.11 The great majority of submitters on our issues paper preferred to leave things as they are. There was certainly no cry for codification. Some of the more interesting arguments in favour of retaining the common law were as follows:
- Codification might upset the balance already achieved by the Broadcasting Standards Authority (BSA) in its complaints jurisdiction under the

²⁴¹ Ibid, ch 4.

²⁴² The arguments for and against codification are presented in *ibid*, paras 7.22-7.34.

Broadcasting Act 1989.²⁴³ If the statute varied from the principles the BSA has adopted, the BSA might feel obliged to change its principles to follow suit. Broadcasters would find that confusing and unsettling.

- Given the small number of decided cases it is too early to codify. Codification is best achieved when there is a lot of material, and in particular a lot of decided cases, to work with.
- Judges are experienced in applying the Bill of Rights Act and in giving proper weight to freedom of information. They are also independent and objective, and immune from political considerations and representations from strong interest groups.
- While it is good to have a tort of invasion of privacy in place, there have been few cases on it (fewer than one a year) and the enactment of a statute would be unlikely to increase that number. The Canadian experience, where there are statutes in four provinces, is that they are very little used. It is not worth expending the resources of Parliament, and the state, in enacting legislation.

We are not saying we necessarily agree with all of these points, but they are certainly of interest.

- 7.12 We noted in our issues paper that the Australian Law Reform Commission has recommended that there be a statutory cause of action for invasion of privacy in that country.²⁴⁴ Since our issues paper was published, the New South Wales Law Reform Commission has also recommended the creation of such a cause of action.²⁴⁵ But the situation in Australia is different, in that there is presently no clearly-established tort at common law. The statute proposed by the Commissions in that country will thus satisfy a need. In New Zealand we do have a common law tort, and we have decided that it should be left to the courts to continue with the task they have begun.
- 7.13 We recommend therefore that the tort be left to develop at common law.

RECOMMENDATION

R28 The tort of invasion of privacy recognised in *Hosking v Runting* should be left to develop at common law.

Partial codification

- 7.14 One submitter suggested that even if the tort were not to be completely codified there might be advantage in codifying some aspects of it. In other words, statute might be able to provide definitive answers to some of the currently uncertain questions and fill some of the existing gaps without codifying all aspects of the tort. We do not support this solution. It can be difficult, even dangerous, to provide answers to only some questions “out of context”, as it were. Partial codification can constrain the development of the common law in the areas which remain its business, and can over time become a “bad fit” with the common law. The United Kingdom Contempt of Court Act 1981, and

243 Ibid, paras 3.36-3.47.

244 Discussed in *ibid*, paras 4.101-4.104.

245 New South Wales Law Reform Commission *Invasion of Privacy* (Report 120, Sydney, 2009).

the New Zealand Defamation Act 1992 and Contractual Mistakes Act 1977 might be thought to fall into that category. Some experiments with composite common law and statute have worked better than this, but in this instance, particularly with the common law in such an early stage of development, we prefer not to proceed down that track.

AN INTRUSION TORT?

- 7.15 The *Hosking* tort is concerned with publicity given to private facts. In some other jurisdictions the tort of invasion of privacy goes further. In the United States, for instance, publicity to private facts is only one of four branches of the tort:²⁴⁶ it is sometimes even said in that country that there are four separate torts. One of them is intrusion into solitude and seclusion and prying into private affairs. This tort is concerned to a significant extent with what we have called spatial privacy, as opposed to informational privacy. It is commonly about invading other people's space by, for example, listening to their conversations with concealed recorders, filming them with hidden cameras, entering their property, or searching their private possessions. Often such invasions occur with the object of getting information, but that is not a necessary element: the invasion is tortious in itself.
- 7.16 Four Canadian provinces have statutory privacy torts:²⁴⁷ all of them extend to this kind of invasion. In New Zealand the Broadcasting Standards Authority (BSA) has long had a privacy principle which deals with "intrusion into solitude and seclusion in the nature of prying" (although since the BSA only has jurisdiction when matter has been broadcast, this principle is inextricably tied up with disclosure of information).²⁴⁸ The Australian Law Reform Commission and the New South Wales Law Reform Commission have both recommended a cause of action which addresses invasions of privacy of all kinds.
- 7.17 In the issues paper we asked whether we should have an intrusion tort in New Zealand.²⁴⁹ We have seen earlier in this report that there is reason for concern in New Zealand about the growth of intrusive technology and the remedies people have or should have against its harmful use.²⁵⁰ In *Hosking* the Court of Appeal left open the question of whether such a tort should be recognised in New Zealand.²⁵¹ So did an earlier High Court case.²⁵² It is the Commission's view that the development of such a tort deserves serious consideration. The real question is whether it should be introduced by statute, or whether it should be left to develop at common law as was the case with the *Hosking* tort. Unlike the *Hosking* tort there is currently no common law on the subject in New Zealand, so there is more of a case to resort to statutory enactment. One of our submitters made a strong case for this. Yet it would be difficult to have one privacy tort existing at common law and the other enshrined in statute. There are obvious links between the two: it is likely, for instance, that any intrusion tort would have a defence of public concern,

246 See Privacy Stage 3 issues paper, above n 232, para 4.8.

247 See *ibid*, paras 4.118-4.129.

248 See *ibid*, para 3.39.

249 *Ibid*, paras 11.30-11.57.

250 See chapter 2.

251 *Hosking v Runtig*, above n 233, para 118.

252 *Marris v TV3 Networks Ltd* (14 October 1991) HC WN CP 754-91 Neazor J.

and it may well be also that there should be a highly offensive requirement. Moreover, in many sets of facts the two torts may both be engaged: as in the case of the media organisation which uses a secret camera to get pictures which it then publishes. The experience of the BSA is that complaints are often based on both the intrusion and the publicity principles.

- 7.18 So the danger in codifying the intrusion tort would be that this could constrain and pre-empt aspects of the common law development of the publicity tort. They are part of one package. In the end, therefore, we have decided to leave the courts to determine whether there should be an intrusion tort, and if so what its ingredients should be. The view of most submitters was that the matter should be left to the courts.

RECOMMENDATION

R29 Any recognition and development of a tort of intrusion into solitude, seclusion and private affairs should be left to the common law.

OTHER CIVIL LIABILITY

- 7.19 As we pointed out in the issues paper,²⁵³ there is another possible avenue of civil liability apart from a tort of invasion of privacy. This is the tort of breach of statutory duty. On occasion the courts will find that a specific duty laid down by statute, perhaps carrying a criminal penalty, is also enforceable by civil action. This is a somewhat precarious and unpredictable course of action: it is said to depend on whether Parliament must have intended the duty to be enforceable by a private action. That boils down to a question of statutory interpretation. One of the principal determinants the courts have used to answer the question is whether the purpose of the provision is to benefit a particular class of the community. But that is not by any means conclusive.
- 7.20 It may well be that a court would find that some statutory duties which currently protect privacy are enforceable in this way. The intimate covert filming provisions of the Crimes Act 1961 may be an example. If a photograph of a woman in an intimate situation, taken without her knowledge, were to appear in a men's magazine, she might well be able to claim compensation by bringing a civil action based on section 216J of the Crimes Act. However, we believe there is merit in making express provision in the case of some of the criminal provisions which currently exist, or are proposed, that as well as constituting criminal offences they are enforceable by civil action. In some instances this may well be simply reinforcing what a court would find already to be the law. But it would remove the need to engage in the difficult and artificial argument which is currently required to succeed in the tort of breach of statutory duty. Nor would any such liability replace the common law tort in *Hosking*. It would supplement it, and might provide a simpler and more direct remedy in appropriate cases.
- 7.21 It is by no means unknown for statute to expressly create a civil cause of action. The Copyright Act 1994 and the Fair Trading Act 1986 are two obvious examples. We have recommended in chapter 3 that the Surveillance Devices Act should expressly provide for a right of civil action in relation to breaches of the criminal provisions of the Act.

²⁵³ Privacy Stage 3 issues paper, above n 232, paras 2.114-2.120.

ANOTHER
TRIBUNAL?

- 7.22 The view has been put to us that we should give consideration to recommending the establishment of a tribunal to administer the tort remedies in privacy. The courts, it was said, are too expensive and sometimes too slow for such a jurisdiction. Moreover, many privacy cases involve intangible loss which may seem better addressed in a lower tribunal rather than through the heavy machinery of a court action.
- 7.23 However, the argument that courts are expensive and slow is not confined to privacy. It can be made of other aspects of the civil jurisdiction. Unless a potential litigant is within the jurisdiction of the Disputes Tribunal, it is often considered not worthwhile to commence an action. So why should we single privacy out? Nor is it true that courts are always slow. Particularly where an injunction is sought they sometimes move with great speed.
- 7.24 In any event there are already avenues of redress for breach of privacy at a level below the court system. Complaints against the media are dealt with by the Broadcasting Standards Authority and the Press Council. As far as complaints against persons other than the media are concerned, the complaints system administered by the Privacy Commissioner under the Privacy Act, which can result in cases going to the Human Rights Review Tribunal, can deal now with complaints about the improper disclosure of personal information and the collection of information by surveillance. As we discussed in chapter 4, we will be putting forward in stage 4 of this Review some proposals for improving and clarifying the Privacy Act's coverage of surveillance.
- 7.25 Privacy Act information privacy principle 11 is capable of dealing with a wide range of disclosures, including dissemination on the internet, while principle 4 can already deal with some instances of intrusion. The statutory exceptions to principle 11 contain ingredients which go some way in the direction of a "public concern" exception, although more confined and specific than the *Hosking* defence.
- 7.26 We think there is currently not a case for *amalgamating* these lower-level complaints-resolution bodies into a privacy tribunal. To do so would involve plucking privacy alone out of the Broadcasting Standards Authority and Press Council jurisdictions. That would not be satisfactory. Privacy is dealt with by those bodies in the wider context of media standards in general. Indeed, privacy often overlaps with other standards such as good taste and fairness, and sometimes complaints are based on several of these standards. To replace the Privacy Commissioner's complaints jurisdiction with a tribunal would be to fundamentally change a system which overall works well.
- 7.27 Nor is there an argument for *adding* a new tribunal to the present range of complaints resolution mechanisms. To add a further layer at the sub-court level would create unnecessary duplication, fragmentation and complexity. Moreover, given the existence of the present complaints mechanisms, it is likely that it would not have much to do. We therefore do not recommend the creation of a specialist privacy tribunal.

Chapter 8

Statutory prohibitions on disclosure

- 8.1 Many statutory provisions in New Zealand prohibit the disclosure of various sorts of information.²⁵⁴ They do not exhibit much consistency.
- 8.2 First, quite a large number of the provisions make it a criminal offence to disclose particular types of information. Among them are Acts prohibiting employees and members of certain government agencies from disclosing personal information which comes into their possession in the course of their employment (tax information,²⁵⁵ remuneration information,²⁵⁶ and information derived from the census,²⁵⁷ for example). Some make it an offence to disclose certain types of health information (information from the cervical cancer screening programme,²⁵⁸ for example). Some prohibit the disclosure of information which has been obtained by illegal surveillance (for example, by interception devices or by intimate covert filming²⁵⁹), or by interception legally undertaken under warrant.²⁶⁰ A provision in the Residential Tenancies Act 1986 makes it an offence to disclose information obtained during a confidential mediation.²⁶¹
- 8.3 Secondly, another group of provisions expressly prohibit disclosure but do not expressly make it an offence. Examples include the Privacy Act 1993²⁶² and the Public Trust Act 2001,²⁶³ which impose such a prohibition on officers and employees, but stop short of expressly imposing a criminal sanction. The Human Assisted Reproductive Technology Act 2004 provides that certain matters, such as information about donors, will not be

254 See New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington, 2009) paras 2.142-2.162 [Privacy Stage 3 issues paper].

255 Tax Administration Act 1994, ss 81, 86, 143C and 143D.

256 Remuneration Authority Act 1977, s 9.

257 Statistics Act 1975, s 21.

258 Health Act 1956, s 112J.

259 Crimes Act 1961, ss 216C, 216J.

260 *Ibid*, s 312K; Misuse of Drugs Amendment Act 1978, s 23.

261 Residential Tenancies Act 1986, s 90.

262 Privacy Act 1993, s 116.

263 Public Trust Act 2001, s 34. Its predecessor, Public Trust Office Act 1957, s 17, did create an offence.

disclosed, but creates no offence.²⁶⁴ Likewise, the Human Rights Act 1993²⁶⁵ makes provision prohibiting the disclosure of information obtained during a confidential mediation, but, unlike the Residential Tenancies Act, does not expressly make such disclosure criminal. It is perhaps arguable that failure to comply with these statutory provisions is an offence by virtue of section 107 of the Crimes Act 1961.²⁶⁶ However, the terms of that section are not straightforward, and it is seldom used. It is all but obsolete. If there are transgressions of provisions of the kind outlined in this paragraph, a complaint under the Privacy Act or internal disciplinary action would seem the most obvious way of dealing with them. Some of the provisions in fact make express reference to the Privacy Act.²⁶⁷

- 8.4 We would note also that there are other enactments which one would perhaps expect to contain provisions prohibiting disclosure but which do not in fact do so. Among them are a number of Acts dealing with sensitive health information which say nothing at all about confidentiality or privacy.²⁶⁸ By leaving matters thus unsaid, the legislators were apparently content to leave the Privacy Act, and the Health Information Privacy Code made under it, to govern the matter.
- 8.5 There are some obvious anomalies. Why is disclosure of mediation information an offence under one Act but not under another? Why is disclosure of some kinds of health information an offence but not other kinds? Why should it be an offence to disclose information obtained by an interception device but not information obtained by unauthorised access to a computer?²⁶⁹
- 8.6 In the issues paper we noted the existence of this mixture of provisions, and wondered whether some coherence could be brought to this branch of the law. We asked three questions in the issues paper. First, are all the present offences required? Secondly, should one take the opportunity of ironing out inconsistencies in the existing criminal offences? And thirdly, do we need any new criminal offences?²⁷⁰
- 8.7 In these enquiries we must bear in mind the complex issue of when it is appropriate to make conduct subject to the criminal law. We have discussed the considerations to be borne in mind in an earlier chapter.²⁷¹

ARE ALL THE
EXISTING
OFFENCES
REQUIRED?

- 8.8 It may well be that some of the existing offences are only offences because they date back to the time before the Privacy Act when there was no other statutory enforcement mechanism available. Those which impose penalties on public officials may also find explanation in the fact that some of them have their origins in the days before the Official Information Act 1982, when the quite different

264 Human Assisted Reproductive Technology Act 2004, ss 51 and 62.

265 Human Rights Act 1993, s 85.

266 The offence of “contravention of statute”.

267 See for example the Human Assisted Reproductive Technology Act 2004, s 66.

268 For example the Intellectual Disability (Compulsory Care and Rehabilitation) Act 2003, and the Human Tissue Act 2008. The Health Research Council Act 1990, although earlier than the Privacy Act, makes no provision either.

269 Crimes Act 1961, s 252: intentionally *accessing* a computer system without authorisation is an offence, but publishing information thus obtained is not.

270 Privacy Stage 3 issues paper, above n 254, paras 7.48-7.54.

271 Chapter 2.

regime of the Official Secrets Act 1951 was in place. Yet we obviously cannot recommend wholesale removal of these criminal sanctions. Some of these prohibitions have underlying policy rationales which go well beyond privacy. Indeed, some of them are probably better described as secrecy or confidentiality provisions rather than privacy provisions. Some are designed to generate trust in government, in that they ensure there will not be misuse of information which citizens have compulsorily supplied for a particular statutory purpose. The tax provisions are designed to secure the integrity of the tax system: indeed, the penalties for infringement in that regime are significant.²⁷²

- 8.9 Each provision therefore would need to be carefully and separately examined before any recommendation was made to render it non-criminal. A review of all of the provisions would be a major exercise which goes beyond the scope of our present project. Yet the current situation does contain anomalies. We recommend that, when next each of the statutes imposing a criminal penalty for disclosing information is reviewed, the question should be addressed of whether the offence provision is necessary, or whether the Privacy Act 1993 provides adequate protection.

RECOMMENDATION

R30 When next each of the statutes imposing a criminal penalty for disclosing information is reviewed, the question should be addressed of whether the offence provision is necessary or whether the Privacy Act 1993 provides adequate protection.

SHOULD THE INCONSISTENCIES WITHIN THE OFFENCE PROVISIONS BE ADDRESSED?

- 8.10 As we noted in the issues paper, there are currently some inconsistencies between the offences themselves.²⁷³ The constituent ingredients of the offence can differ between one offence and another. The defences are different between Acts. Sometimes there are discrepancies in the penalties. As far as the offences of disclosing material obtained under interception warrants are concerned, these will be attended to in the Search and Surveillance Bill currently before Parliament. Likewise, if the Surveillance Devices Bill that we recommend in this report is enacted, further discrepancies will be removed. In so far as other provisions are concerned, we recommend that whenever one of the statutes which imposes a penalty for disclosure of information is reviewed and it is decided to retain the offence provision, attention should be paid to its consistency with analogous provisions.

RECOMMENDATION

R31 Whenever one of the statutes which imposes a penalty for disclosure of information is reviewed, attention should be paid to its consistency with analogous provisions.

²⁷² Tax Administration Act 1994, ss 143C and 143D (added in 1996).

²⁷³ Privacy Stage 3 issues paper, above n 254, para 7.53.

ARE ANY NEW
OFFENCES
REQUIRED?

- 8.11 We considered whether there are any further breaches of privacy which are so serious that it is in the public interest that they should carry a criminal penalty. Some of those who made submissions on the issues paper believed that this question deserves serious inquiry, although the submissions did not exhibit much unanimity as to what those offences might be.
- 8.12 We have noted that criminal offences should not be created lightly, but we have made recommendations for offences related to disclosure in chapter 3 on the proposed Surveillance Devices Act. Our recommendations are based on the principle that if a particular means of acquiring information is an offence, then it should be an offence to publish information knowing it was so acquired. Thus, we have recommended that it should be an offence to knowingly publish information acquired by unlawful visual surveillance, tracking and interception.
- 8.13 We have also considered whether there should be an extension of the disclosure offences relating to intimate covert filming. At the moment it is only an offence to publish intimate pictures of someone if they were taken covertly and without consent. If the taking of the picture was with consent, subsequent publication of it without consent is not an offence. We have wondered whether it should be made so under the proposed Surveillance Devices Act. We have in mind as an example the case where a film is taken with consent in the course of an intimate relationship, but later when the relationship breaks up the film is distributed far and wide,²⁷⁴ perhaps even posted on the internet. To render such conduct criminal under the proposed legislation would be to create an exception to our general principle that the disclosure offences should mirror the interception and surveillance offences, and after due deliberation we have decided that there is not sufficient justification for doing so. If the film comes within the definition of “objectionable publication” in the Films, Videos and Publications Classification Act 1993 – and if it is sexually explicit it may do so – disclosure of it will be an offence under that Act. Beyond that, we think the matter is a civil one. Being filmed without consent is different in kind from being filmed with consent: the latter must always involve the subject in an element of personal risk. The abuse of the relationship of trust and confidence involved is more appropriately dealt with, we believe, through civil avenues that are already available. In our issues paper on the review of the Privacy Act we shall also be suggesting ways in which the “domestic affairs” exception in that Act may be narrowed so that it does not protect conduct of the kind we are considering. In the questions we put for public submission on our website talklaw.co.nz in the course of our research for this report, we had a scenario of exactly the kind we are now considering; 5 out of 6 people who commented on that scenario thought that criminalisation would be going too far.
- 8.14 We foreshadow also that we shall be considering further offences in our review of the Privacy Act 1993. An issues paper on that stage of our privacy project is being published early in 2010. It may be desirable to add an offence to the Privacy Act relating to obtaining access to information by impersonation or misrepresentation. That will be discussed in the issues paper.

274 The Victorian case of *Giller v Procopets* [2008] VSCA 236 provides an illustration.

- 8.15 There may also be some egregious forms of disclosure of health information which may merit criminal sanction. One of our submitters gave the example of releasing all the information attached to National Health Index numbers to a third party. We have already noted in this chapter the anomalies in the law relating to health information. A few types of disclosure are already subject to criminal penalty, but others are left to the Privacy Act 1993 and the Health Information Privacy Code. We believe that the whole area of health information needs separate review. We shall return to this issue in the fourth stage of our Review.



Appendices



Appendix A

Some further issues relating to interception

In chapter 3 we recommend that further work be undertaken to assess the adequacy of the criminal law framework in relation to the interception of electronic communications. We have identified the following issues that require examination:


- The relationship between the interception offence and the computer misuse offences:
 - (a) Is the interception offence limited to electronic communications between people?
 - (b) Do the computer misuse offences extend to the interception of electronic communications?
- Whether the reasonable expectation of privacy enquiry is a necessary generic requirement in relation to all forms of communications, or whether it can be targeted at particular forms of communications.
- Whether the enactment of a further offence of accessing stored communications is necessary.

RELATIONSHIP BETWEEN THE OFFENCES OF INTERCEPTION AND COMPUTER MISUSE

We have considered the interplay between the interception offence and the computer misuse offences²⁷⁵ in relation to electronic communications and telecommunications. Depending on the circumstances, the interception of electronic communications could fall under either the interception offence or the computer misuse offences or both.²⁷⁶ Increasing technological convergence means that there is now potentially greater overlap between the two offences in relation to telecommunications. The interception of telecommunications originally fell exclusively within the interception offence, but as mobile phones and telecommunication devices have become multi-functional, the interception

²⁷⁵ Crimes Act 1961, ss 248-254.

²⁷⁶ Maximum penalties of two years' imprisonment are consistent as between the interception offence (Crimes Act 1961, s 216B) and the unauthorised computer access offence (Crimes Act 1961, s 252).



of telecommunications could also now fall within the ambit of the computer misuse offences.²⁷⁷ The interception of email is potentially covered by both the interception offence and the computer misuse offences.²⁷⁸

The boundaries and areas of overlap between the interception and computer misuse offences are not altogether clear. To the extent that there is an overlap, this may not matter, as the computer misuse offences could act as back-up offences in relation to interceptions of electronic communications that are not “private communications”. On the other hand, the fact that the interception offence was specifically amended in 2003 to include electronic messages, together with various uncertainties around interception under the computer misuse offences, could lead to the interception offence being interpreted as the definitive offence relating to interception, to the exclusion of the computer misuse offences.²⁷⁹

Two questions for further consideration are whether the interception offence is limited to the interception of communications between people, and to what extent the computer misuse offences cover the interception of electronic communications. It is necessary to resolve these issues to clarify whether the interception of categories of electronic communication such as human-to-computer communications and data transmissions between computers are covered by the criminal law, or whether there are any gaps in the current legal framework for the interception of electronic communications.

The scope of the interception offence is relevant when considering practices such as deep packet inspection. This is a form of network packet filtering that can assist service providers to monitor traffic loads and manage network performance. Overseas, however, some service providers have been involved in ventures to use this technology to monitor user communications and internet activity for commercial purposes.²⁸⁰ To the extent that the interception offence applies, practices that exceed the specific service provider exception (for maintenance of the network) will be unlawful. However, such practices will not be unlawful to the extent that the interception offence does not apply to them.²⁸¹

277 Where interception is achieved through computer hacking.

278 This is subject to the issues raised further below.

279 The implicit coverage of interception in the New Zealand computer misuse offences can be compared with explicit data interception offences in Singapore (Computer Misuse Act 1993, s 6) and Canada (Criminal Code RSC 1985 c C-46, s 342(1)(b)). See also the data surveillance device offences in New South Wales (Surveillance Devices Act 2007, s 10); Victoria (Surveillance Devices Act 1999, s 9); Northern Territory (Surveillance Devices Act 2007, s 14).

280 See Paul Ohm “The Rise and Fall of Invasive ISP Surveillance” [2009] U Ill L Rev 1417, 1426.

281 The topic of deep packet inspection will also be considered in the Law Commission’s issues paper on reform of the Privacy Act.

Are private electronic communications limited to communications between people?

The interception offence covers communications in electronic form. Electronic communications now take a variety of forms including email, electronic data interchange, “chat room” correspondence, instant messaging, mobile phone calls and messaging, PDA communications and landline telephone calls.²⁸² One question is whether the communications covered by the interception offence are limited to communications between people, such as emails and text messages, or whether they include a wider range of electronic communications, such as communications between a person and a computer or data transmissions between computers:²⁸³

only a small fraction of the Internet’s traffic involves human-to-human communications such as email messages. Most Internet communications are communications between humans and computers, such as World-Wide-Web pages in transit, commands sent to remote servers, and file transfers. Many others are computer-to-computer communications, such as network administrative traffic that keeps the Internet running smoothly.

We think that the stronger argument is that the New Zealand interception offence is limited to communications between people, based on the explanatory note to Supplementary Order Paper 2000 No 85, and the definition of “party” in section 216A(2) of the Crimes Act 1961. However, we note that a broader view of a “communication” was taken by the House of Lords in *Morgans v Director of Public Prosecutions*,²⁸⁴ where the use of a call-logging device that captured digits dialled, both before and after connection to a telephone line, was found to intercept a communication. The call-logger provided evidence that the appellant had fraudulently accessed a telecommunications system to make calls free of charge.²⁸⁵

In the United States, the interception offence extends to the interception of electronic communications, defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature.” The courts have held the following activities to be within the scope of the offence: copying emails before they are delivered, obtaining a cookie from a customer’s computer, and installing and using spyware to capture chat conversations, instant messages, emails and websites visited.²⁸⁶ The inclusion of a specific exception to the interception

282 New South Wales Law Reform Commission *Privacy Legislation in New South Wales* (CP 3, Sydney, 2008) para 5.97.

283 Orin S Kerr “Internet Surveillance Law After the USA Patriot Act: the Big Brother That Isn’t” (2003) 97 Northwest U L Rev 607, 613; see also 662 [“Internet Surveillance Law After the USA Patriot Act”]. See also Steven Penney “Updating Canada’s Communications Surveillance Laws: Privacy and Security in the Digital Age” (2008) 12 Can Crim L Rev 115, 152-153: “Person-to-computer communications... are not ‘communications’ in the conventional sense of the word, and give rise to a distinct set of privacy and crime control concerns that are deserving of separate consideration by Parliament and the courts.”

284 *Morgans v Director of Public Prosecutions* [2000] 2 All ER 522, 537-539.

285 See “Internet Surveillance Law After the USA Patriot Act”, above n 283, 646 (n 191).

286 Ohm, above 280, 1478.

offence to allow for the monitoring of the activities of computer hackers²⁸⁷ suggests that the United States interception offence covers human-to-computer communications such as hacker commands.²⁸⁸

To what extent do the computer misuse offences cover the interception of electronic communications?

The potential scope of the computer misuse offences is broader than the interception offence, as these offences may cover electronic messages between people as well as a broader range of electronic communications, such as transmissions of data between computers. However, the extent to which the computer misuse offences cover interception is not expressly stated in the Crimes Act. One question is whether the interception of data is an aspect of “access”.²⁸⁹ Prior to the enactment of the computer misuse offences,²⁹⁰ the Law Commission recommended the enactment of a specific computer misuse offence for the unauthorised interception of computer data, as well as offences for unauthorised access, use and damage.²⁹¹ However, it was considered that the unauthorised computer access offences would be broad enough to include the interception of computer data.²⁹² “Access” is broadly defined to mean “instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of a computer system”.²⁹³

This interpretation is consistent with an exception to the unauthorised access offence in section 252 of the Crimes Act, for access to a computer system by a law enforcement agency under an interception warrant. However, there is some further uncertainty about the scope of the computer misuse offences which turns on the meaning of “interconnected”, as used in the definition of “computer system”.²⁹⁴ If a “computer system” is essentially a network under the common control of a person or entity, the offence of accessing a computer system without authorisation should cover the interception of data as it is sent within the network. But it is less clear that the offence covers the interception of data as it is sent between computer networks.

Nevertheless, where the interception of data necessitates access to a network (for example, to install a keystroke logger or malware), we note that the computer misuse offences would cover this aspect of the hacking operation.²⁹⁵

287 18 USC. § 2511(2)(i).

288 “Internet Surveillance Law After the USA Patriot Act”, above n 283, 665-671.

289 For discussion of the term “access”, see Orin S Kerr “Cybercrime’s Scope: Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” (2003) 78 NYU L Rev 1596.

290 The computer misuse offences as enacted drew on the 1991 recommendations of the Crimes Consultative Committee.

291 New Zealand Law Commission *Computer Misuse* (NZLC R54, Wellington, 1999) para 90. The proposed interception offence was intended to cover activities such as packet sniffing: see *ibid*, para 18.

292 Letter from Ministry of Justice to the Law Commission, 15 July 1999.

293 Crimes Act 1961, s 248. One anomaly noted in Hon J Bruce Robertson (ed) *Adams on Criminal Law* (loose leaf, Brookers, Wellington, Crimes Act, 1992) para CA252.01 [*Adams on Criminal Law*] is that the definitions in section 248 do not extend to the offence of unauthorised access created by section 252.

294 Crimes Act 1961, s 248. See discussion in *Adams on Criminal Law*, above n 293, para CA248.03; David Harvey *internet.law.nz* (2 ed, Wellington, LexisNexis, 2005) 211.

295 See Wade H Baker, C David Hylender and J Andrew Valentine 2009 *Data Breach Investigations Supplemental Report* (Verizon Business, 2009).

REASONABLE
EXPECTATION
OF PRIVACY
AND DIFFERENT
MODES OF
COMMUNICATION

In chapter 3 we query whether the reasonable expectation of privacy test is a necessary component of the interception offence as it relates to electronic communications, and whether it should be omitted or modified in some contexts. In our view it would be desirable to limit the operation of the reasonable expectation of privacy test to the methods of communication in which the test is useful for identifying which communications are protected from interception and which are not. The problem with a generic application of the test is that it raises doubts as to whether various forms of communication are protected from interception until such time as there may be judicial confirmation of the expectation of privacy and the scope of the interception offence's protection.

We note that in Australia, the interception of telecommunications (including messages) does not incorporate a privacy-expectation-based threshold,²⁹⁶ nor is the threshold used for the interception of electronic communications under the United States Electronic Communications Privacy Act.²⁹⁷ In the United Kingdom, the interception offence in the Regulation of Investigatory Powers Act 2000 targets the interception of telecommunications without including a reasonable expectation of privacy test. In Canada, however, the offence of interception of telecommunications is subject to a test that there was a reasonable expectation that the communication would not be intercepted.²⁹⁸

We do not anticipate that removing the reasonable expectation of privacy test for certain forms of electronic communication would have a significant impact on law enforcement agencies by requiring significantly higher numbers of interception warrants to intercept private communications. Generally, we would expect that law enforcement agencies currently obtain warrants to intercept emails and text messages. The removal of the privacy-expectation criteria from these forms of communications is therefore unlikely to have a material impact on law enforcement operations. However, the reform would provide greater certainty to the public that communications by email and text message are considered to be private communications and should not be subjected to unauthorised interception.

The difficulty is that there is no clear boundary that can be drawn delineating which forms of communication require the application of the test. Some forms of electronic communication have commonalities with oral communications (suggesting that application of the reasonable expectation of privacy test is desirable), while other forms of electronic communication are more akin to posted mail or computer misuse (suggesting that the test is unnecessary). One United States commentator suggests that in the online context, a reasonable expectation of privacy should presumptively protect the content of internet communications, but leave non-content information (related to identity, location and time) unprotected.²⁹⁹

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

297 18 USC § 2510. The test is used for the interception of oral communications.

298 Criminal Code RSC 1985 c C-46, ss 183-184.

299 Orin S Kerr "Applying the Fourth Amendment to the Internet: A General Approach" (forthcoming) Stan L Rev. See also Ohm, above n 280, 1453, discussing the complexities of the content/non-content distinction in relation to email.

Clarification of the relative scope of the interception and computer misuse offences, as discussed above, would assist to identify the type of electronic communications at issue so that a specific assessment of the role and nature of the privacy-expectation enquiry in relation to electronic communications can be carried out.

Oral communications

We have reached the view that a privacy-expectation assessment is necessary for the regulation of the interception of oral communications, including oral conversations between people in person, oral conversations by telephone and oral communications using other communication channels (such as radiocommunications and internet communications).³⁰⁰ In this context, criteria are necessary to identify which spoken conversations between people may be intercepted legitimately (for example, the taping of comments at seminars, press conferences and interviews or public meetings) and which conversations may not be intercepted without consent.

In the case of telephone conversations, there are a range of circumstances in which conversations (or one side of a conversation) may be overheard: for example, calls may be played on speaker phone and additional parties may be linked in to conference calls. Telephone calls are not confined to private places but can be made from anywhere, including highly public places. A privacy-expectation assessment assists to focus the protection of the interception offence on those communications that are intended to be confined to the parties themselves.

It could be argued that discarding the privacy expectation enquiry in relation to oral conversations by telephone would not make the interception offence overbroad on the basis that:

- (i) the interception offence is limited to interception using an interception device and therefore does not extend to overhearing conversations without the use of a device; and
- (ii) the participant monitoring exception provides sufficient flexibility to permit third parties to listen to or record telephone conversations with the express or implied consent of one of parties to the conversation.

However, we think that the privacy expectation enquiry provides a further useful criterion to delimit the scope of the interception offence in relation to oral communications.

300 Internet telephony or Voice over Internet Protocol (VoIP) represents the convergence of oral communications and data transmissions. The treatment of these communications as oral communications should be assessed under the recommended review of the framework for the interception of electronic communications. For a comparison of regulatory issues in the EU and US, see Daniel B Garrie and Rebecca Wong "Privacy in Electronic Communications: the Regulation of VoIP in the EU and the United States" [2009] CTLR 139. See also Jeremy Malcolm "Privacy Issues with VoIP Telephony" (2005) 2(2) Priv LB 25; Pat Pilcher "Who is Listening to Your Skype Calls?" (8 September 2009) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 17 September 2009).

There are certain communication channels, such as citizen band (CB) radio, that are notoriously insecure; privacy expectations of users of such channels are either absent or much lower than for other communication channels. One option is to continue to use a privacy-expectation test to exclude these communications from the ambit of the interception offence.

Alternatively, a more tailored or specific requirement could be adopted in place of the reasonable expectation of privacy test. For example, in Canada, to deal with the uncertain position of early cellphone communications, a specific amendment was made to the definition of “private communication” to include “any radio-based telephone communication” and to apply a different privacy-expectation formulation based on whether the communication has been treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the intended recipient.³⁰¹ This means that any security measures by carriers to encrypt or otherwise protect communication channels, even if not perfect, will qualify communications using those channels as “private.”³⁰² The United States Code also deals specifically with radiocommunications by providing an exception to the interception offence for communications that are “readily accessible to the general public”.³⁰³ We think that there is merit in making it explicitly clear that readily accessible radiocommunications are presumptively excluded from being “private communications.”³⁰⁴

Electronic communications

For some forms of electronic communications, such as email and text messages, we think that the desirability of the privacy-expectation criterion is less clear-cut. Parties using these communication channels desire or expect the communication to be confined to the parties to it in the first instance. Although parties to text messages and emails generally assume the risk that the other party may subsequently forward a message to a wider audience, this does not extend to an expectation that messages will be intercepted by third-party outsiders as they are being transmitted.³⁰⁵

Another form of electronic communication is instant messaging over the internet, allowing groups of people to communicate in real time. This form of real-time communication has similarities to telephone voice communications,³⁰⁶ but is also another form of written communication. Internet chat communication is a particular feature of child pornography offending and is therefore a source of information and evidence to law enforcement investigators.

301 Criminal Code RSC 1985 c C-46, s 183. See also s 184.5 which criminalises the interception of any radio-based telephone communication (whether or not a private communication) where this is done maliciously or for gain.

302 Penney, above n 283, 123-125.

303 18 USC § 2511(2)(g).

304 For a definition of radiocommunications that are “readily accessible to the general public”, see for example 18 USC § 2510(16).

305 See, however, Penney, above n 283, 134-135, comparing the relative privacy expectations in relation to email and voice communications. See also Patricia L Bellia “Surveillance Law Through Cyberlaw’s Lens” (2004) 72 Geo Wash L Rev 1375, 1385-1386.

306 Penney, above n 283, 135, noting that differences between voice and text communications are rapidly eroding.

The privacy expectation of parties to internet “chat” will vary depending on whether the platform used is a public site or a private forum. The privacy expectation criteria may therefore be useful to target the prohibition on interception to those communications that are intended to be private.³⁰⁷ However, the participant monitoring exception that permits a person to record or intercept communications to which he or she is a party may be broad enough to permit law enforcement officers to gather information and evidence from these sources.³⁰⁸ If so, it may not be necessary to retain the privacy expectation enquiry in this context.

As noted above, one inconsistency between the interception offence and the computer misuse offences is that the computer misuse offences do not rely on a privacy-expectation threshold.³⁰⁹ If both the interception and computer misuse offences cover the interception of computer data, it seems unnecessary for the interception offence to use the reasonable expectation of privacy threshold while the computer misuse offence does not.³¹⁰ Alternatively, if the interception offence covers the field of electronic interception, it seems inconsistent for the privacy expectation threshold to apply in the case of interception but not to the accessing of stored data under the computer misuse offences. On balance, we think that there is a case for a more coherent framework for the interception of electronic communications. The question for further consideration is whether the offences can be rationalised by removing the privacy expectation enquiry from the interception offence as it applies to electronic communications.

Postal mail

Besides electronic communications, the other form of written communication that is capable of being intercepted is communications sent by post. Interception of the mail is not dealt with by the interception offence; there are specific offences in the Postal Services Act 1998 dealing with the opening of other people’s mail and the disclosure of its contents.³¹¹ The offence for opening other people’s mail does not involve an enquiry into privacy expectations but creates a presumption that communications by mail are private and are eligible for the protection of the offence on a generic basis.

307 See, for example, *R v Kwok* [2008] OJ No 2414 Gorewich J.

308 See cases cited by Bellia, above n 305, fn 193.

309 Crimes Act 1961, ss 248–254. Other distinctions between the two types of offence are (a) the requirement of the interception offence that interception be achieved through use of an interception device is not a requirement of the computer misuse offences; and (b) the restriction on disclosure of unlawfully-intercepted communications in s 216C does not extend to disclosure of unlawfully-accessed material or information under the computer misuse offences.

310 For example, the interception of a series of text messages between cellphones, one of which could be categorised as a “computer” due to its applications and one of which is solely a communications device, may be treated differently under the different offences.

311 Postal Services Act 1998, ss 20, 23. The interception of mail is dealt with by law enforcement agencies under the search warrant procedure rather than the interception warrant procedure. There would also be scope for law enforcement agencies to use production orders in relation to postal articles under the provisions of the Search and Surveillance Bill 2009, no 45-1, part 3, subpart 2. By way of comparison, in the United Kingdom, the interception of telecommunications and postal communications is covered by the Regulation of Investigatory Powers Act 2000, part 1, chapter 1. This Act provides for a warrant procedure for the interception of both forms of communication.

Visual surveillance and the interception of communications

The definitions of “private communication”, “intercept” and “interception device” are broad enough to encompass the visual surveillance of communications by filming or watching (with the assistance of a device) an oral conversation between people that can then be interpreted through lip-reading, or communications using sign language or other hand signals. Another scenario is the use of visual surveillance devices or hidden cameras to monitor computer screens as a means of capturing communications such as emails.

We conclude that the reasonable expectation of privacy test is a necessary element of the interception offence in relation to the visual surveillance of communications. Communications conveyed visually by means such as sign language can be made in a variety of public and private contexts, and we think that they should be treated in a similar manner to oral communications. For the use of visual surveillance to intercept digital or electronic communications, however, there is a question as to whether the privacy expectation test is needed, or whether this should be a form of computer misuse that does not rely on the privacy expectation test.

ACCESSING STORED COMMUNICATIONS

A further question is whether the interception offence and computer misuse offences are sufficient to protect electronic communications from illegitimate access. While it is a crime to acquire private electronic communications through interception or computer hacking, it is not otherwise an offence to obtain private electronic communications after they have been sent, where this is achieved without committing a computer misuse offence. For example, an employee of a service provider could copy and read all emails stored in a client’s inbox,³¹² or users of a computer system with shared access could breach the terms of their authorisation and access one user’s stored private communications.³¹³

Jurisdictions such as Australia³¹⁴ and the United States³¹⁵ have enacted offences against accessing stored communications, subject to certain exceptions to allow for search warrants and other necessary access. Both the Australian and United States offences specifically protect communications held by service providers, and neither offence depends on the parties to the communication having a reasonable expectation of privacy in it. The United States has two tiers of offence: the first is where the offence is committed for commercial advantage, malicious destruction or damage, or private commercial gain or in furtherance of a criminal or tortious act;³¹⁶ while the second is where the offence is committed in any other case.³¹⁷ One Canadian commentator has recommended that access to stored communications in that jurisdiction be criminalised when carried out “maliciously or for gain.”³¹⁸

312 Penney, above n 283, 138.

313 This is an exception to computer misuse under s 252(2) of the Crimes Act 1961.

314 Telecommunications (Interception and Access) Act 1979 (Cth), s 108.

315 Stored Communications Act 18 USC §§ 2701-2712 (2007) (Title II). The offence has been interpreted as being limited to the accessing of “unopened” communications: see Bellia, above n 305, 1415. There is also an exception to the offence for access by service providers, see 18 USC § 2701(c)(1).

316 Stored Communications Act 18 USC §§ 2701(b)(1).

317 Ibid, §§ 2701(b)(2).

318 Penney, above n 283, 142.

In New Zealand, there are statutory limits on internet service providers and communication service providers intercepting private communications.³¹⁹ The remaining question is whether similar limits should be placed on accessing stored communications, including limits on use and disclosure. Options for creating an offence of accessing stored communications include:

- an offence based on whether a person has a reasonable expectation of privacy in the stored communications;
- an offence that protects stored communications in the custody of service providers that offer an internet or communications service to the public; and
- an offence that turns on intent, such as where stored communications are accessed “maliciously or for gain”.

Our preference is for the second option that targets the storage of communications by service providers. While private communications are currently protected from interception by service providers (subject to an exception for maintaining services), we think that there should be complementary protection at the point of storage. This would cover both access instigated by a service provider and unauthorised access by service provider employees (who may otherwise be exempted under section 252(2) of the Crimes Act). The offence would need to include any appropriate exceptions, including a warrant exception for law enforcement officers requiring access to stored communications for investigative purposes. The offence would preclude the voluntary supply of communication content by service providers to law enforcement agencies in the absence of a warrant or production order.³²⁰

Apart from this, we do not think that the exemption for persons who are authorised to access a computer system in section 252(2) of the Crimes Act should be altered. “Insiders” who access computer systems for inappropriate purposes should remain subject to civil law remedies (such as the Privacy Act) and private sanctions (such as employment policies and contract terms).

319 Crimes Act 1961, s 216B(5).

320 See *R v Cox* (2004) 21 CRNZ 1 (CA).

Appendix B

Tort of invasion of privacy: analysis of submissions

In the issues paper we asked a series of questions about the elements of the *Hosking* tort and about gaps in the tort as it has developed so far. We sought views on how these elements should be developed and how the gaps should be filled if the tort were to be codified in statute. We also asked about these issues in relation to the possibility of developing an intrusion tort. This appendix summarises the responses to these questions in the submissions we received.


1. Should the “highly offensive” test remain as a separate element of the tort?

There was a fairly equal division on whether the “highly offensive” threshold should be maintained. Those who supported it noted that it was justified by the high importance of freedom of expression and that it would stop fanciful claims. It also applies to the *publicity* rather than to the facts in respect of which there is an expectation of privacy. One submitter noted that its retention enables the blameworthiness of the defendant to be considered, as well as the expectations of privacy of the plaintiff. She also felt that “highly offensive” focuses on community standards more explicitly than does “reasonable expectation”.

Those who opposed the two-part test said that any invasion of a reasonable expectation of privacy is objectionable per se; and, furthermore, that “highly offensive” introduces too great an element of subjectivity. Some said it set the threshold too high. One person thought that “offensive” is not the right word in any event; rather, the question is whether a reasonable person would be “distressed” or “humiliated”.

2. Is “reasonable expectation of privacy” a useful test? Would it be possible in a statute to give more precise definition, or to list considerations to be taken into account in determining whether that expectation exists?

There was fairly general support for the “reasonable expectation of privacy” test. One submitter noted that it has precedent in other jurisdictions,



and that it is elastic and can evolve, thus making it well-suited to privacy jurisprudence. Most felt that spelling out a list of examples or criteria would be difficult, and could be too constraining. It would be dangerous to try to predict what might happen in the future. Ultimately, each case will depend on its own facts. However, a small number of submitters felt that a list of examples might be of some help, provided it was quite clear that it was non-exhaustive. One submitter listed factors which might be helpful (including the nature of the material disseminated, whether the plaintiff is a public figure, and whether the claimant has courted publicity); but thought it would be dangerous to identify categories of private information – for example, medical and financial information – because there are degrees of sensitivity within categories. The New Zealand Law Society made the interesting suggestion that it might be more useful to spell out a set of examples where there is *no* reasonable expectation of privacy: previous court proceedings where a person’s name has not been suppressed, for example.

One interesting view was that “reasonable *expectation*” is not the best test, because if media behaviour becomes increasingly intrusive one in fact comes to expect less and less privacy. Rather, it was said, the test should be “reasonable *desire*” for privacy.

3. In what circumstances can there be a reasonable expectation of privacy in relation to things which happen in a public place? Is it possible to devise a test to clarify this issue?

Some submitters from the media tended to think that there can be nothing private about what happens in a public place. As one said, “an expectation of privacy in a public place defies logic.” But they did note that, if the matter arises, editors exercise their discretion, and are influenced by considerations of good taste when making decisions in this difficult area.

Most submitters thought, however, that while one has reduced expectations of privacy in a public place, there could be exceptional cases where publicity would be offensive. They would include situations where:

- the plaintiff’s conduct was unplanned and not reasonably to be expected (the example was given of a woman giving birth);
- technology such as hidden or long-range cameras, or devices to penetrate clothing, was used;
- vulnerable people, such as mentally impaired or very young persons, were involved; or
- the plaintiff was in a place where he or she reasonably believed he or she could not be seen.

Some submitters thought that plaintiff culpability should be relevant, and that those who commit unlawful or anti-social behaviour in a public place should not reasonably expect privacy. One submitter thought that it would be

difficult to legislate, but believed that the public place cases were ones where the “highly offensive” criterion can be particularly useful. Another warned that any attempt to legislate here “would stray into an extremely dangerous grey area.”

4. To what extent is the degree of privacy that public figures can reasonably expect less than that of the general population? Does any reduced expectation of privacy on the part of public figures also apply to their families?

There was general agreement that public figures have a lesser expectation of privacy: “The more widely known they are, the less privacy they can reasonably expect.” But it was noted that there are different sorts of public figures. A person who is reluctantly thrust into the public eye (for example, the victim of a crime or accident) should not forfeit privacy. A person who voluntarily gets involved in a news story, for example by being a whistle blower, or a person who has the good fortune to be an actor or sportsperson well known to the public, must obviously expect more attention than others, but should not on that account forfeit the right to keep his or her private life private. It might be different, however, if the public figure actively sought media attention; then something like a waiver might operate. Those who benefit from a positive media image have less ground for complaint when the media give the other side of the story. Even then, however, such a person is entitled to some residual area of privacy on sensitive matters, and to be free from intrusions into the home. But if public figures’ private lives are relevant to their occupations or public roles, they must expect less privacy with regard to those aspects. Those in public office have reduced privacy rights, particularly regarding things which reflect on their integrity.

As far as the families of public figures are concerned, there was a general view that they have as much right to privacy as anyone else. Young people should not be subjected to humiliating publicity just because their parents are well-known. The younger they are, the greater that expectation of privacy. Nevertheless, there may be exceptions where a young person likely to inherit a public role from his or her parents might excite a legitimate degree of public attention: members of the Royal Family might be an example. Again, if family members get involved in matters of public concern, such as criminal behaviour, in their own right, their privacy will be correspondingly decreased. Likewise, where information about a person’s family reveals hypocrisy on the part of the public figure, or where a family member’s personal circumstances may affect the public figure’s conduct of his or her job, there would be a case for publication. The Privacy Commissioner believed that the public concern defence covers most elements of this subject. One submitter from the media industry thought there was no need to legislate: “New Zealand does not have the paparazzi and highly self-obsessed celebrity culture” of some other countries.

5. In what circumstances can there be a reasonable expectation of privacy in relation to something which has already been published?

There was a difference of opinion on the extent to which matter already published could continue to be the subject of a privacy claim. Some thought that, once information has been published, all privacy has gone with respect to

that information, and noted that the retention of material in databases and their potential long-term searchability was changing expectations in this regard. But others felt that it depended on the circumstances. One said, for example, that a politician should not have to be pilloried because of a high school stunt which took place many years ago. One submission said it should depend on the following matters:

- the sensitivity of the information (some very humiliating information should not become public property just because it has been published once);
- the length of time involved since the previous publication;
- the extent of the first publication;
- the original intended audience (intended publication to a small group of friends on Facebook does not mean the information should be available to be viewed by the whole world);
- the public interest considerations at the time and now; and
- the effect on the person concerned.

Another submission said that, in relation to such things as a Facebook page, the age of the author or publicist is relevant. The New Zealand Law Society thought that elements of the law of contract and breach of confidence might be used by way of analogy: to whom the information was disclosed, and on what basis, should influence the extent to which the subsequent publication is actionable.

6. At what time should the expectation of privacy be assessed: the time of the occurrence of the facts in question, or the time of their projected publication?

The majority of submitters thought that publication was the relevant time, although a few believed that depending on circumstances it could be either the time the information was created or the time it was published.

7. How far should plaintiff culpability be relevant to reasonable expectation of privacy? Is it possible to frame a statutory test to deal with plaintiff culpability?

Almost all submitters thought plaintiff culpability was in some way relevant, but that it would be difficult to lay down a clear test. One thought that the very idea of “plaintiff culpability” is not helpful because it is shorthand for a number of different concepts. The following matters were thought to be relevant:

- how far the complainant’s conduct amounted to a crime, or was otherwise against the public interest;
- whether the complainant himself or herself initially created the publicity;
- whether the plaintiff had made misleading statements which justified refutation;
- whether the complainant was reckless in releasing private facts; and
- whether the culpable behaviour occurred in a public place.

One submitter made the point that if culpable behaviour is only suspected, rather than proven, the question becomes much more difficult. Another thought that plaintiff culpability went to the “highly offensive” criterion rather than “reasonable expectation”. Perhaps, once again, public concern is the overriding

criterion. The New Zealand Law Society noted that the difficulty of incorporating culpability into any comprehensive test may be another reason for leaving this tort to develop at common law.

8. Would it be helpful, in a statute, to give examples of matters which are normally of legitimate public concern?

Three submitters thought it would be helpful, and one was attracted to the Broadcasting Standards Authority list in *Balfour v Television New Zealand Ltd*,³²¹ but it was noted that any attempted formulation would have to state clearly that the examples given were not exhaustive. The majority of submitters, though, thought it would not be wise to give criteria or examples in statute for fear that they could be (i) too confining, thus closing the door to the unusual case or further development, or (ii) too broad, thus expanding the defence too widely. The Screen Production and Development Association (SPADA) noted that any attempt to “list” factors might prejudice the advice in *Andrews* that one should not strip reports of all attendant colour and detail.

9. Should the statute require only reasonable grounds for belief that the matter is of legitimate public concern, or should the test be an objective one?

There was near unanimity that the objective test was the correct one. But one submitter thought that there might be a difference according to whether the question was (i) whether the matter was of public concern or (ii) whether a particular item was *relevant* to that matter of public concern.

10. Other than “legitimate public concern”, what defences should there be to a cause of action for publicity given to private facts?

Some possibilities for other defences suggested by submitters were consent, Parliamentary privilege, qualified privilege, contributory negligence, triviality, the fact that the information is already in the public domain, fair comment and the fact that publicity is necessary to counter selective facts put into the public domain by the complainant. (A number of these so-called defences are probably better dealt with as ingredients of the cause of action, and can be readily absorbed into the “reasonable expectation” and “highly offensive” tests.)

11. What remedies should be available?

Most believed that injunction and damages should remain the main two remedies. However, one submitter suggested there might be merit in considering further remedies such as return of documents, account of profits and publication of a correction. The last of these would obviously only apply in cases where the information published was inaccurate. The analogy to defamation was noted. Another submitter recommended that remedies should be consistent with those available through the BSA and the Privacy Act. There was little enthusiasm for exemplary damages, although one submitter believed strongly that they

321 *Balfour v Television New Zealand Ltd* (21 March 2006) Broadcasting Standards Authority 2005-129, para 59.

should be available, because they are available in other torts which involve insult – for example, assault and defamation – and have even been extended to negligence.

12. Is it possible, or desirable, to list considerations to be taken into account in assessing damages?

There was a division of views on this, although even those who supported listing factors were concerned that it might act as a constraint. The New Zealand Law Society thought that the damages regime should be aligned with statutory remedies in other statutes, such as the Privacy Act: “If the regimes apply different standards and awards it will distort litigant behaviour”. The same submitter made the point that the plaintiff should choose a single forum: a defendant should not have to face proceedings in the Human Rights Review Tribunal, the Broadcasting Standards Authority and the District Court over the same matter.

13. Should it be possible to obtain a remedy in this privacy tort if some or all of the statements made about the plaintiff are untrue?

Most submitters thought not, and that inaccuracy was the province of defamation rather than privacy. That, however, was not the universal view. One said a privacy action should not be ruled out just because a few facts in an article are untrue. The Privacy Commissioner’s Office noted that in the context of information privacy laws it is quite usual for privacy cases to involve a mix of true and false statements about an individual. Nevertheless, they noted that a practical solution would be needed as to whether defamation or privacy was to be pleaded, and in what circumstances. One submitter thought the question was whether the *gist* of the information is true: if the essence of the complaint is about spreading false information, defamation is the cause of action. Another thought it was important that privacy not be used to circumvent the rules of defamation.

14. Should wide publicity be required to ground a cause of action or might publication to a small group be enough in some cases?

All submitters thought that there could be cases where damage could be done by disclosure to a small group of people, and that therefore wide publicity was not necessary. Sometimes it is communication to one’s immediate circle that one most wishes to avoid. However, one submitter thought that would be exceptional, and that the “highly offensive” test might control the issue. Another made the interesting point that it may be that the essence of the cause of action should be the harmful misuse of private information, and that wide publicity would be only one subset of that.

15. Should it ever be possible to obtain a remedy for invasion of the privacy of a deceased person?

A few submitters thought yes, at least if the disclosures had an adverse effect on the deceased’s family. One was particularly concerned about the depiction of a deceased person’s body. But the majority thought not. One believed that remedial action is the essence of the tort, and if the subject is dead it is too late for remedy.

Another said that privacy is closely tied to the effect on individuals, and there is little merit in conducting an action when the subject is dead. Another felt that it would be unprincipled to have a different rule for privacy than exists for defamation.

16. Should corporations, or other artificial persons, be able to bring an action for invasion of privacy?

Only two submitters thought corporations can have privacy. Otherwise there was unanimity that, since privacy protects human dignity, corporations are not eligible. One submitter who thought that the question deserved more consideration gave as an instance the stigma which would attach to bodies corporate if past “leaky building” history could be revived and republished.

17. Is it possible to lay down a statutory test to clarify the special position of children?

All submitters recognised the particular vulnerability of children. Members of the media noted that the privacy of children is specially covered by media codes. Some submitters agreed with the BSA provision that even if the parents consent to a broadcast about children, the broadcaster must also exercise judgment as to whether the broadcast is in the best interests of the children. One broadcaster commented that that may be too high a test and that what is really meant is that the broadcast should not *harm* the interests of the children. The New Zealand Law Society thought it would be very complicated and difficult to put an appropriate test into words, and that, as was recognised in *Hosking v Runting*, the vulnerability of children can be taken into account in the offensiveness and “reasonable expectation of privacy” criteria. It can be taken into account also in the measure of damages.

18. Might it ever be possible for a person to succeed in an action for publicity given to private facts if that person was not identified in that publicity? To whom would the person need to be identified?

Most submitters believed that the plaintiff needs to be identified. A number pointed out that identification does not need to be express, provided that there are indicators in the publication which can lead to identification. The Privacy Commissioner noted that it might even be possible to create that identification by combining one publication with another. However, three submitters disagreed, and thought identification may not be necessary in all cases. One gave the example of a person who is paraded naked through a public place, but with a bag over the person’s head to prevent identification: it was suggested that that person should have a remedy in tort.

19. What mental element should be required to found liability in a defendant?

Most thought that intention was necessary, and that there should be a defence for innocent disseminators. One submitter said there were two questions: the first relates to the *fact* of publication, and the second to whether the publisher has knowledge of the plaintiff’s desire for privacy, and that the requirements might be different for each.

20. If there is to be an intrusion tort, what should be its elements? Should it be limited to intrusions into spatial privacy, or should it include intrusions into personal affairs? Would it differ from the disclosure tort in relation to any of the questions listed above?

Most submitters thought an intrusion tort should cover both spatial privacy and intrusions into personal affairs (which relate more to informational privacy). On the whole, submitters thought that the answers to the other questions above would be the same with respect to the disclosure and the intrusion torts. A couple of submitters suggested that freedom of expression may not be an issue to the same extent in intrusion cases as in disclosure cases, and that this could have implications for matters such as the “highly offensive” threshold and the legitimate public concern defence.

This document was printed on Novatech Paper. This is an environmentally friendly stock that originates from sustainable well managed forests. Produced at Nordland Papier paper mill, which holds both FSC and PEFC chain of custody certificates. (Reg. No. SGS-COC-2249) ISO 14001 environmental management systems certified. The mill is registered under the EU Eco-management and Audit Scheme EMAS. (Reg. No.D – 162 – 00007). The paper bleaching process is Elemental Chlorine Free, and Acid Free.

The HIT Pantone inks used in production of this report are vegetable oil based with only 2 percent mineral content, and are created from 100% renewable resources. The wash used with these inks was Bottcherin 6003, which is entirely CFC and Aromatic free.



