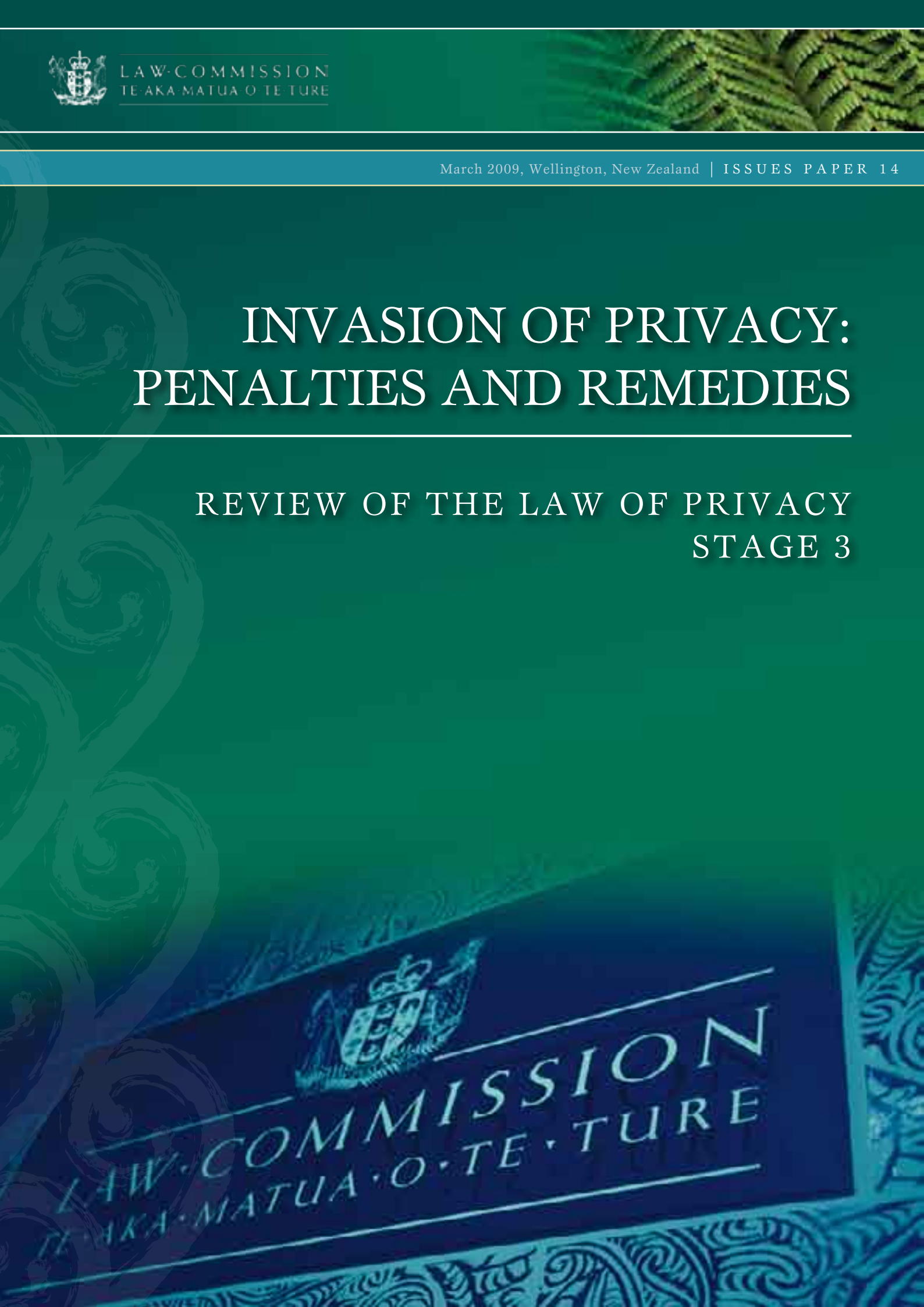
LAW COMMISSION
TE AKA MATUA O TE TURE

March 2009, Wellington, New Zealand | ISSUES PAPER 14

INVASION OF PRIVACY: PENALTIES AND REMEDIES

REVIEW OF THE LAW OF PRIVACY STAGE 3



LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

March 2009, Wellington, New Zealand | ISSUES PAPER 14

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.
(Issues paper ; 14)
ISBN 978-1-877316-66-1
1. Privacy, Right of—New Zealand.
I. New Zealand. Law Commission.
II. Series: Issues paper (New Zealand. Law Commission) ; 14.
342.930858—dc 22

ISBN: 978-1-877316-66-1 (Print)
ISBN: 978-1-877316-67-8 (Online)

ISSN: 1178-2862 (Print)
ISSN: 1177-7877 (Online)

This paper may be cited as NZLC IP14

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

FOREWORD

The Commission's project on privacy has four parts. A study paper and a report have already been published. This issues paper deals with what has proved to be the most difficult aspect of the Commission's terms of reference – in particular, the tort of privacy and questions relating to surveillance. A great many difficult issues are canvassed in this paper and many questions are asked. The Commission needs clear answers from members of the public and people who may be affected by any changes in the law that could come from our final report. There are important issues at stake on both sides of many of the issues raised in this paper. We want to hear from every side and as many people as possible. We have found doing the work and formulating the issues a big challenge. We do not yet know where the answers lie. We need help.

We would like to thank the Office of the Privacy Commissioner and the Ministry of Justice for their continuing cooperation with this Review.

Sir Geoffrey Palmer
President

Call for submissions

Submissions or comments on this issues paper should be sent to the Law Commission by **Friday 29 May 2009**.

Privacy submissions
Law Commission
PO Box 2590
Wellington 6140

email – privacy@lawcom.govt.nz

Any enquiries may be made to ***Ewan Morris*** **04 914 4821**.

There are questions set out in various chapters of this issues paper, and collected at the end of the paper, on which we would welcome your views. It is not necessary to answer all questions. Your submission or comment may be set out in any format, but it is helpful to indicate the number of the question you are discussing, or the paragraph of the issues paper to which you are referring.

This issues paper is available on the Law Commission's website www.lawcom.govt.nz

Official Information Act

The Law Commission's processes are essentially public, and it is subject to the Official Information Act 1982. Thus copies of submissions made to the Law Commission will normally be made available on request, and the Commission may refer to submissions in its reports. Any requests for withholding of information on grounds of confidentiality or for any other reason will be determined in accordance with the Official Information Act 1982.

Invasion of Privacy: Penalties and Remedies

CONTENTS

Summary

1 Privacy is an issue of interest and importance to everyone. The value we place on it has increased in recent times in proportion to the rise of increasingly sophisticated means of invading it. The issues raised in this paper are of significance to ordinary people.

THE EXISTING LAW IN NEW ZEALAND

2 The main focus of this issues paper is the adequacy of both New Zealand's civil law, and its criminal law, to deal with invasions of privacy. But we have found it necessary to examine these sanctions and remedies in the context of the various modes of regulation which exist. It is not practicable to discuss only some modes of enforcement in isolation. Chapter 2 outlines the ways in which privacy is currently enforceable in the courts in New Zealand. We deal first with civil remedies whereby a citizen can sue either for damages or an injunction. For a long time there have been various causes of action which protect privacy indirectly. They include breach of confidence; harassment; malicious falsehood; trespass (to land, goods or person); defamation; breach of contract; and passing off. Some of them are ancient causes of action. Each of them primarily protects an interest other than privacy, but is sometimes capable of protecting privacy as well. We also note the existence of a tort of breach of statutory duty, one of our more uncertain torts, which sometimes may be used to give a civil right of action for breach of a statutory provision.

3 However, in recent years there has been growing authority in New Zealand that there is a separate tort of invasion of privacy which gives a cause of action if publicity is given to private facts about someone, where that publicity is highly offensive to a reasonable objective person. In *Hosking v Runting* it was decided by a bare majority in the Court of Appeal that there is indeed such a tort. A member of the Supreme Court has later indicated that the very existence of the tort may require re-examination, but currently it must be taken to be law in New Zealand. We describe the tort only briefly in chapter 2. We proceed later in the paper to analyse and discuss it in more detail.

4 As far as the criminal law is concerned, there are many statutory provisions which to some degree protect privacy. They are scattered over a large number of Acts of Parliament. There is little coherence about them, and they do not cover anything like the whole field. They are in fact a strangely patchy and ad hoc collection. Moreover, quite a number of them, rather like the specific torts of which we have just spoken, protect privacy only tangentially: the rules about the secrecy of the ballot, for example, protect the integrity of our electoral system just as much as the privacy of the voter.

5 In addition to enforcement through the courts, there are a number of other ways of enforcing privacy in New Zealand. The Privacy Act 1993 lays down a number of information privacy principles. This Act is principally concerned with the way agencies collect and store information about people, the security of that information and how it is to be used. Those who are affected by a breach of the principles in the Act can complain to the Privacy Commissioner; if they do not obtain a satisfactory resolution, the matter can proceed to the Human Rights Review Tribunal. The media are exempt from most of the provisions of the Privacy Act if they are engaging in news activities.

6 The Broadcasting Act 1989 provides that all broadcasters must observe standards which are consistent with the privacy of the individual. Complaints about the breach of these standards can be made to the Broadcasting Standards Authority, which in the course of its complaints jurisdiction has formulated a number of privacy principles. It can impose sanctions, and in particular it can make awards of damages for privacy breaches. The Press Council deals with complaints against the print media. It occasionally hears privacy complaints. Its jurisdiction is not statutory, and it cannot impose legal sanctions. The Advertising Standards Authority is also a voluntary body with a limited jurisdiction over privacy matters. Other relevant regulatory frameworks are those established by the Health and Disability Commissioner Act 1994 and the Unsolicited Electronic Messages Act 2007, and certain industry self-regulatory codes.

THE LAW IN OVERSEAS JURISDICTIONS

7 In chapter 4 we outline the position in other jurisdictions with regard to privacy law. In most of the countries we examined there is an array of statutes and common law rather like our own, and in all of them there is also a regulatory framework which is not dissimilar from ours. In these other jurisdictions there is not much more coherence than we find in our own.

8 We note in particular that there has been a privacy tort in the United States for many years. It can be broken down into a number of distinct categories. The *Hosking* tort, which is about publicity given to private facts, mirrors one of the United States categories. Plaintiffs have not been very successful in that country, particularly when suing media defendants.

9 In England, the courts have been developing a cause of action which is not unlike the *Hosking* tort, but they have done so under the influence of the European Convention on Human Rights, and rather than creating a new tort they have preferred to do much the same job by extending the law on breach of confidence. The English courts are also influenced by the jurisprudence of the European courts. There are a growing number of cases in England, and they are likely to be cited in New Zealand. However, we would caution that the legal and constitutional contexts of the two countries are rather different. A different path again has been taken in the Republic of Ireland, where the courts have recognised a cause of action for invasion of privacy by finding an implied privacy right in the Constitution.

10 So far the Australian courts have not definitively endorsed a tort of invasion of privacy, although that possibility has been left open by the High Court of Australia. The Australian Law Reform Commission has recommended a statutory cause of action for breach of privacy, but that has not been positively received in some quarters. In Canada, likewise, there has been no clear endorsement of a common law tort, although there is a statutory tort of invasion of privacy in four of the provinces. That statutory tort goes wider than *Hosking v Runting* in that it applies to intrusions beyond just publicising private facts. However, there has been very little litigation, and in such as there has been plaintiffs have often been unsuccessful.

CONCLUSIONS ON THE CURRENT LEGAL POSITION

11 In chapter 5 we sum up the present state of our New Zealand law. We conclude that, while it offers some protection for privacy interests, the law is piecemeal, and there are some significant gaps and anomalies. In particular, surveillance and intrusion are not comprehensively covered by any of the current modes of enforcement. We note also that some areas of the law, in particular the *Hosking* tort, are beset by uncertainty and open-ended concepts.

12 We discuss briefly the respective spheres of the criminal and civil law, and the practical considerations which may dictate which of them serves best in particular situations. We note that their spheres of operation can occasionally overlap. By and large, the lower-level modes of enforcement (the Privacy Commissioner, the Human Rights Review Tribunal, the Broadcasting Standards Authority and the Press Council) offer cheaper and speedier modes of redress. There may be merit in investigating whether they, or bodies like them, might play a greater role in the privacy arena rather than relying on the heavy and expensive machinery of the courts.

DISCLOSURE OF PERSONAL INFORMATION

13 In Part 2 of the paper we deal with the protection our law gives against the offensive disclosures of private facts about people. Most of the discussion in this part is about the *Hosking* tort. The elements of that tort are as follows: (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 will be considered highly offensive to an objective reasonable person. There is a defence enabling publication to be justified by legitimate public concern in that information.

14 The tort has sometimes been said to be based on the inherent dignity of the human being. That raises some difficulties. Dignity may not be the only interest protected: it is fairly clear that financial loss, for example, and even danger to personal safety may be compensated under this tort. Insofar as dignity is an important basis, there are questions as to how one measures damage to it, and places a value on that loss. Our common law courts are not experienced in assessing damage of this kind. The new tort has close links with breach of confidence, and the boundaries between the two will need to be worked out. There will doubtless be cases where a plaintiff could sue in either in the alternative.

15 The elements of the tort as stated above are open-ended. "Reasonable expectation of privacy" is a broad expression which will involve the exercise of judgement in each particular case. It is clear that it goes well beyond facts which are intimately personal, and extends to other matters which it is reasonable to expect will be kept private. Until there have been a number of cases which set precedents, it will be difficult to chart its exact scope. To that extent, the law will not be readily predictable. The expression "reasonable expectation of privacy"

raises some difficult questions. Can one have a reasonable expectation of privacy in a public place? To what extent do public figures and celebrities have an expectation of privacy? How far can there be a reasonable expectation of privacy in material which has already been published? Can the culpability of the plaintiff ever reduce or negate the expectation of privacy?

16 The "highly offensive" criterion also raises questions. Some have wondered whether it should be a separate criterion at all, or whether it is just a factor to be taken into account in deciding whether there was a reasonable expectation of privacy in respect of the facts of the case. However, it is clear that the test has been introduced to ensure that only the most serious cases come within the purview of the court. That is necessary if the tort is not to unreasonably limit freedom of expression. It should also be noted that the "highly offensive" test relates not just to the facts in question but also to the nature and extent of the publicity about them. Assuming that the highly offensive test remains part of our law, it also raises questions of judgement and impression. Different people can sometimes differ on its application to a particular set of facts.

17 The defence of legitimate public concern ensures that a balance is drawn between the interest in privacy and the interest in the free flow of information. Once again, "legitimate public concern" is not susceptible of clear definition, although it is a concept with which our courts have become fairly familiar in other contexts. It adds yet another layer of uncertainty. The remedies available under the tort according to the judges in *Hosking* are damages and injunction. We have already alluded to the difficulty of assessing damages for harms to dignity. Injunction, it is said, is an exceptional remedy, although the considerations applicable in a privacy case may well not be quite the same as those which arise in other cases, such as defamation, where freedom of information is at stake.

18 In addition to all these uncertainties there are also gaps in the tort which, if it remains a common law tort, will have to be filled by the courts on a case-by-case basis. Such cases may take a long time to arise, and there are quite a number of gaps to be filled. Are there any other remedies? Are there any other defences? What is the relationship between invasion of privacy and defamation? Does the tort require wide publicity or will publication to only one other person suffice? Can corporations sue as well as individual persons? Can the tort protect the dignity of dead people as well as the living? Is any mental element required? Does the plaintiff have to be identified, and if so to how many people?

19 In the light of these uncertainties and gaps, is reform required? We discuss this in chapter 7, and pose some questions on which we seek the views of the public. Given the existence of other ways of enforcing privacy, for example through the Privacy Act and the Broadcasting Standards Authority, we ask whether we need the tort at all. We look at the arguments for and against the tort. Assuming the tort was to disappear, however, should it be replaced by something else? If so, would that be done by extending the powers of some of the regulators, or by creating a kind of lower-level law enforceable in a tribunal? If it is decided to retain the tort, the question is whether it should be left to be developed by the common law, a slow process, or whether it should be codified in statute. Both of these solutions have their advantages and disadvantages. The common law can keep in touch with reality. It is also flexible, and can move with the

times. On the other hand, statute does not have to wait for cases as they arise; it can provide answers and fill the obvious gaps from the outset. The process of statute-making also allows for wide consultation of affected interests. If it is decided that there should be a statutory tort, there is then a question as to what its content should be. We ask questions about that.

20 The discussion of the disclosure tort is the main topic in Part 2. We also ask, however, whether anything needs to be done to rationalise the present criminal offences relating to disclosure of personal information: whether they are all necessary; whether others should be added; and whether any inconsistencies and anomalies in them should be eliminated. We also ask whether there would be merit in providing expressly by statute for a civil remedy for the breach of some of the criminal provisions. Provisions expressly allowing for a civil remedy for breach of a statute would grant more certainty than is currently available.

SURVEILLANCE: BACKGROUND

21 In Part 3 we examine surveillance and other forms of intrusive conduct. Surveillance we define as the use of devices intentionally to monitor, observe or record people's actions or communications. It can take a variety of forms, including observing, listening to, watching, recording, or otherwise collecting information about people. One of the most common forms of surveillance is closed-circuit television (CCTV), but there are many other types: radio frequency identification (RFID) tags, audio recording, photography, and tracking devices such as Global Positioning System (GPS) locators. Some types of data monitoring, such as the use of spyware, are also included in our discussion.

22 There can be a number of reasons why people might wish to undertake surveillance, and some of them are quite legitimate. They include gathering evidence of wrong-doing, deterring wrong-doing such as theft or speeding, monitoring performance (say, in a workplace), determining the preferences of customers in a store, or monitoring a young child or an infirm person at home. Other purposes are totally unacceptable: voyeurism, for example.

23 Surveillance can take place in a public or private place. While, generally speaking, surveillance in a public place is less problematic, it should not be assumed that it is always acceptable. People in public places do not give up all their expectations of privacy, particularly if they are caught in a vulnerable situation not of their own making, and there can also be important questions as to the use to which the information collected is put, how long it is stored, and who has access to it. There is also a distinction between targeted and mass surveillance, the one being focussed on an identifiable person or persons, the other casting the net more widely. Another distinction is between covert and overt surveillance. Covert surveillance occurs secretly, without the knowledge of the subjects, while overt surveillance takes place openly with the subjects' knowledge, or at least with notice having been given that surveillance is taking place. Generally, overt surveillance is the less intrusive mode, but it would be wrong to conclude that it is free of problems: few people would be comfortable if they knew they were being watched all the time, particularly when they are on private property. We acknowledge that this distinction between overt and covert surveillance is imperfect: for example a person can sometimes be unaware of the presence of closed-circuit television cameras even though no attempt has been made to conceal them. Surveillance, whether overt or covert, can have negative effects: the chilling effect of being watched, loss of anonymity, stress and

emotional harm, insecurity, and loss of trust are among them. Moreover, sometimes more information is gathered than is within the original purpose of the surveillance, and as we have said, there can be concerns as to what use is made of it afterwards.

THE CURRENT LAW ON SURVEILLANCE

24 In chapter 9 we outline the current law relating to surveillance. Some parts of the existing civil law cover aspects of surveillance: trespass and harassment, for example. The *Hosking* tort has limited application, for it only comes into play if there is *publication* of information thus obtained. In a few instances the tort of breach of statutory duty may be able to be pressed into action, although it is not clear exactly when that will be available. The Privacy Act information privacy principles can have some application insofar as they relate to the collection of information, although in our view the application of these principles to surveillance is not as clear as should desirably be the case.

25 The Broadcasting Standards Authority has developed a principle relating to intrusion into solitude and seclusion. A number of its privacy complaints have been decided on that basis. However, since the BSA only deals with complaints about programmes which have been broadcast, the principle is as much about *publication* as it is about surveillance pure and simple.

26 The criminal law is limited and patchy in its application. Some of its provisions proscribe covert activity such as the secret filming of people in intimate situations, and the interception of communications by audio recording devices or other types of interception device. Computer hacking and unauthorised access to computers are also covered. Some more overt types of surveillance can also sometimes fall foul of the criminal law: some of the provisions of the Harassment Act, and the prohibition on private investigators taking photographs or making recordings, for instance.

27 It is as yet undetermined whether some forms of surveillance by public agencies (CCTV for instance) could engage section 21 of the Bill of Rights Act (unreasonable search and seizure.)

28 A number of situations are not covered well, or indeed at all, by our existing legal provisions. We give a number of example scenarios where the law may be unclear or less than satisfactory: for example, filming through the window of a dwelling house; a person installing a rooftop camera trained on his neighbour's backyard; the use of software which allows the user to activate a webcam attached to someone else's personal computer; cellphone monitoring; and a CCTV camera which captures and stores pictures of an amorous couple in a public place.

SURVEILLANCE LAW REFORM OPTIONS

29 In chapter 10 we examine the possibilities for reform of the law as it relates to surveillance. They include civil liability which mirrors and complements the criminal offences (in other words, breach of statutory duty). We consider the introduction of a new tort which might stand alongside the *Hosking* publicity tort: this might go wider than surveillance per se, and cover intrusion of all kinds. Any such tort would have to be clearly delimited, and be subject to a public concern defence. We ask whether the criminal law protections should be expanded or supplemented, and whether any such criminal provisions should be general in nature, or instead limited in particular ways: for example, limited to the use of specific kinds of device. We examine specific solutions in some detail,

and summarise the solutions arrived at in some of the Australian states. We ask what sorts of exceptions and defences should apply, and whether participant monitoring should continue to be a defence to the interception offences (as it currently is in the interception provisions of the Crimes Act.)

30 Other options are to amend the current Privacy Act principles so that they more explicitly cover surveillance, or to add a new set of surveillance principles, as the New South Wales Law Reform Commission has recommended. There is also the option of controlling activities such as CCTV through various regulatory mechanisms. These might include legislation regulating CCTV, either through a separate Act or an addition to the Local Government Act 2002. Other possibilities might include a code of practice, or a set of standards. Any such reforms might deal with such questions as who may engage in surveillance in public, either by CCTV or otherwise; the purpose for which it can be undertaken; the use which can be made of the images obtained; access to the records kept; requirements as to giving notice; and the use of techniques which are fair.

INTRUSION INTO SECLUSION AND PRIVATE AFFAIRS

31 There are other forms of intrusion in addition to surveillance. We deal with these in chapter 11. The phrase, which originated in the United States, of "intrusion into solitude and seclusion" largely captures this concept. Examples include physical intrusions into spaces where a person could reasonably expect to be left alone; searches of private spaces such as rooms, vehicles or lockers; access to personal objects such as bags, diaries, cellphones or email; bodily searches; and the sustained watching of other people (peeping-tom activity) without the use of devices. We again provide example scenarios where the law currently is unclear or unsatisfactory, among them an example based on the English case of *Kaye v Robertson* where media personnel gained entry to a hospital room and conducted an interview with a seriously ill man.

32 We ask whether the existing civil and criminal law should be extended. Some of it is currently narrow. For example, the offence of peeping and peering into a dwellinghouse applies only at night; and the Harassment Act 1997 requires a pattern of conduct and not just an isolated incident. Is there a need to extend the ambit of any of these provisions?

33 We also ask whether there should be an intrusion tort as a companion to the publicity tort of *Hosking v Runting*. We examine the arguments for and against having such a tort: we ask whether, if there is to be such a tort, it should be introduced by statute rather than being left to the common law to develop; and, if there should be a statute, what it should contain. The last matter involves such questions as whether the definition of the elements of the tort should require intrusion into "solitude or seclusion", which might suggest that it can have no application in public spaces; and also whether it should be confined to intrusion into physical space, or rather go beyond that and include prying into personal affairs. There are questions as to how general or how specific any definition might be, and whether any legislation might include examples or lists of factors to be taken into account, both with respect to the elements of the tort and any defence of public concern that there might be. We also ask, as we did in relation to the *Hosking* tort, whether another solution might be to introduce a machinery for dealing with privacy intrusions at a lower level than the court.

THE MEDIA, THE WORKPLACE, AND PRIVATE INVESTIGATORS

34 Chapter 12 is concerned with surveillance and intrusion in relation to three specific sectors: the media, the workplace, and the private investigation industry. We do this because these sectors raise particular challenges in terms of balancing privacy with legitimate public and business interests, and also because there is a question whether the laws which currently govern them need further consideration.

35 The media sometimes use surveillance techniques such as hidden cameras. They also sometimes use material obtained by surveillance undertaken by others. The media in their news activities are excluded from the coverage of the Privacy Act 1993. Complaints about their conduct may be made to the BSA, which has statutory authority, and the Press Council, which does not. The BSA has stated that there is a presumption that hidden filming will be unfair unless there are overriding public interest factors. It has found that the use of hidden cameras will usually be an intentional interference with solitude or seclusion in the nature of prying for the purpose of their Privacy Principle 3. The media, of course, are also subject to the general law relating to interception, trespass and so on. Media personnel tell us that they are currently uncertain what their rights and obligations are, in particular when filming in a public place.

36 Any privacy rules applying to the media must strike a proper balance between the protection of privacy and freedom of information. The media play a vital role in informing the public about issues of public importance. Any restrictions on the ways in which they can gather information will be a limit on the freedom to seek, receive and impart information and opinions under the Bill of Rights Act, and will therefore need to be reasonable and demonstrably justifiable in a democratic society. We ask whether the media should be subject to different legal constraints from anyone else, and whether the current framework of regulation is adequate. We also ask what form any exceptions for the media should take.

37 The workplace involves balancing the legitimate entitlement of employees to a degree of personal privacy with the interests of the employer in running an efficient and safe workplace. Currently, workplace surveillance is to some extent covered by the Privacy Act and the general provisions of the criminal and civil law, although as we have seen, those protections are somewhat patchy. In addition, it is governed by aspects of employment law such as procedural protections, and the obligations of trust, confidence and good faith. Some commentators have noted a number of areas where reform might be considered, such as alcohol and drug testing and the monitoring of off-duty conduct. Such commentators wonder whether there needs to be closer regulation. We ask whether the current legal protections are adequate, or whether there should be a specific statute governing workplace surveillance (as there is in at least one Australian state) or a privacy code.

38 Currently, private investigators are required to be licensed, and there is a presumption against licensing them if they have been convicted of an interception offence under the Crimes Act in the past five years. Moreover, it is an offence under section 52 of the Private Investigators and Security Guards Act 1974 for a private investigator to take or use any photograph, film or video recording of a person, or to record a person's voice without prior written consent. This is a prohibition which applies to no other sector of society. There are anomalies in

the provision: it applies only to private investigators and not to security guards, nor does it prohibit the use of other surveillance equipment such as tracking devices. We ask whether it is right that private investigators should be subject to specific legal controls that do not apply to other members of the community (as is currently the case under section 52), and whether surveillance activities by that profession should be regulated in some other way; for example, by a code.

CONCLUSION

39 Chapter 13 is an overview chapter which highlights the difficulties we have identified in the paper and the problems of the current law. It also summarises the fundamental questions we need to address in any reform exercise. In particular we discuss the respective roles of the criminal and civil law, and regulation. We also note that, while some overlap between the various sanctions is sometimes inevitable, it is also important that the law should be as coherent and consistent as possible, taking into account, however, the differences between the varying situations in which privacy issues can arise. We note the matters which must be weighed in the balance with privacy: the public interest, the rights and freedoms in the Bill of Rights Act, and compliance costs.

40 We seek input from the public. We hope that input will come from a wide range of people, and represent as many different points of view as possible.

Chapter 1
Introduction

THE LAW COMMISSION'S REVIEW OF PRIVACY

1.1 This issues paper seeks public submissions on stage 3 of the Law Commission's 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 will inform 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.

1.3 The Commission will be producing an issues paper on stage 4 of the Review later this year, and calling for submissions on the issues raised in that paper. Because the Privacy Act is the subject of a separate stage of our Review, we do not focus on it in this stage 3 issues paper. At the same time, the Act inevitably looms large in any discussion of privacy law, and we have not been able to ignore it in our consideration of the issues raised by stage 3. At various points in this issues paper we discuss the Act, and in some places we have asked questions about how the Act might be used to address certain issues. Reform of the Privacy Act spills over into wider issues of reform of the law relating to privacy more generally. When we come to produce our final reports for stages 3 and 4, we will have the benefit of considering submissions on the issues papers for both stages, and will be able to consider how our recommendations for each stage will affect the other.

---

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).

STRUCTURE AND APPROACH OF THIS ISSUES PAPER

1.4 Part 1 of the issues paper looks at the existing legal position. We discuss enforcement of privacy in the New Zealand courts, through civil remedies and criminal offences, and at the framework of the Privacy Act, the various bodies that regulate the media, and other regulatory frameworks (chapters 2 and 3). We also examine privacy law in a number of other jurisdictions: the United States, Europe, the United Kingdom,[3] Ireland, Australia and Canada (chapter 4). In chapter 5 we draw some general conclusions about the current state of New Zealand law, and the lessons that can be learned from overseas.

1.5 In parts 2 and 3 we turn to options for reform of the law. The division of material between these two sections is partly based on a distinction between two different types of privacy which we drew in *Privacy: Concepts and Issues*. In that study paper we distinguished between informational privacy, which "is concerned with control over access to private information or facts about ourselves", and *spatial (or local) privacy*, which "is concerned with access to our persons and to private spaces".[4] We have found this distinction useful, but it is not the only basis on which we have structured parts 2 and 3. Equally important is the distinction between disclosure of private information and the means by which private information is obtained.

1.6 Part 2 of this issues paper is about the disclosure of private facts, and is thus clearly focused on informational privacy. The bulk of Part 2 is concerned with the tort of invasion of privacy by publicity given to private facts. This tort was found to exist in New Zealand common law by the Court of Appeal in the case of *Hosking v Runting*,[5] and we therefore refer to it as the *Hosking* tort. Chapter 6 looks at the nature of the *Hosking* tort, and identifies areas of uncertainty relating to the tort. We then look at options for reforming the tort in the first part of chapter 7, including the questions of whether there should be a tort at all, and whether it should be common law or statutory. The second part of chapter 7 considers whether there are any other gaps in the law relating to disclosure of private information that should be filled.

1.7 In Part 3 we examine some complex issues relating to intrusions into individuals' solitude or seclusion and prying into their private affairs. A particular focus of Part 3 is the use of surveillance. The issue of intrusion cuts across our distinction between informational and spatial privacy. Many intrusions involve interferences with spatial privacy: physical intrusions into private spaces, opening and searching of personal possessions, watching or listening to others without their knowledge or consent, and so on. Such activities can interfere with people's reasonable expectations of spatial privacy, regardless of whether any significant information is obtained as a result, or of whether that information is particularly private in nature. Often, however, intrusions will result in sensitive, private information about a person being discovered. This is also an interference

3 A major report on surveillance and privacy issues in the United Kingdom was released too late to be considered in this issues paper: House of Lords, Select Committee on the Constitution "Surveillance: Citizens and the State" (HL 18, 2009).

4 New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) 57, 59.

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

with informational privacy. While Part 2 is concerned with the disclosure of private information, one of the areas of concern in Part 3 is the obtaining of private information (which may or may not be disclosed further).

1.8 The first three chapters of Part 3 focus on surveillance, which is one of the most significant types of intrusion. In chapter 8 we define surveillance for the purposes of our discussion as "the use of devices intentionally to monitor, observe or record people's actions or communications". Chapter 8 provides background information on surveillance, including how surveillance is used, some of its negative effects, and public attitudes towards it. Chapter 9 sets out the current law relating to surveillance, while chapter 10 considers options for civil, criminal and regulatory law reform. Chapter 11 broadens the discussion out to the wider issue of intrusion, and in particular considers the option of a tort of invasion of privacy by intrusion into seclusion or private affairs. We conclude Part 3 with a consideration of issues relating to surveillance and other forms of intrusion in three particular sectors: the media, employment and the private investigation industry.

1.9 Part 3 is concerned with matters that are relatively novel and unexplored in New Zealand law. For this reason, Part 3 is somewhat longer and more detailed than Part 2. It also employs a technique of illustrating the scope of the current law, and gaps in the law, with reference to hypothetical scenarios. We hope that this technique will assist readers in understanding the issues and assessing whether or not there are gaps in the law that should be filled.

1.10 The final chapter of this issues paper draws together the threads of all three parts, summing up some of the difficulties and issues that the paper has identified.

SUBMISSIONS

1.11 Details of how to make a submission are at the front of the issues paper. We welcome submissions in any form, but we encourage submitters to address the questions we have asked throughout the paper. These questions vary greatly in their level of specificity. Some are quite general, while others address particular points of law. The more detailed questions are included mainly for those with particular expertise or areas of interest, and we do not want other members of the public to be deterred from putting their views forward by the number of questions or the specificity of some of them. It is not necessary to answer all of the questions, and we invite submitters to answer as many or as few as they wish. It will be as useful to the Commission to hear in general terms what form the law should take as it will be to hear views on the specific details of the law.

1.12 Following receipt of the submissions we will prepare our final report, with recommendations to the government for reform of the law.

Part 1
EXISTING LEGAL POSITION

Chapter 2

Enforcement in the courts

2.1 Privacy interests are given both direct and indirect protection by a variety of civil and criminal remedies in New Zealand. These are described in this chapter. As will be seen, these remedies tend to protect privacy in a piecemeal and arguably inadequate manner: it cannot be said that their development has been guided by a principled or systematic appraisal of privacy values. The New Zealand Bill of Rights Act 1990 also provides protection for some privacy interests, but it does not recognise a free-standing right to privacy.

CIVIL REMEDIES

2.2 The most significant civil remedy is the relatively new and distinct action for wrongful publication of private information, affirmed by a majority of the New Zealand Court of Appeal in *Hosking v Runting*. This section examines the development of that tort and its application since *Hosking*. It also describes the position under the New Zealand Bill of Rights Act. At the end of the section, we describe the other civil remedies that can be said to protect various privacy interests. These other remedies have grown up through the development of the common law as it applies to the protection of more tangible concerns such as property, trade and reputation.

Wrongful publication of private facts – early developments

2.3 Over the last 30 years, the New Zealand courts have become increasingly aware of privacy as a value. For example, in *Auckland Medical Aid Trust v Taylor*,[6] where a search warrant was declared to be unlawful for failing to specify the particular offence under investigation, McCarthy P said:

> In my view, it would be contrary to the role which the Courts of our tradition have always adopted of protecting the integrity of a man's premises and of viewing in a conservative way the extension of statutory powers to interfere with privacy, if we were to uphold the warrant in this case.

6 *Auckland Medical Aid Trust v Taylor* [1975] 1 NZLR 728, 737 (CA). See also *R v Jefferies* [1994] 1 NZLR 290 (CA); *R v Fraser* [1997] 2 NZLR 442 (CA). See John Burrows "Invasion of Privacy" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) para 18.2.02.

2.4 In *Moulton v Police*, the Court of Appeal gave consideration to the police power to obtain information necessary to identify an arrested person:[7]

> Of course it does not follow that, in the guise of asking for particulars, the police may delve into a person's past. In a sense, details of a person's schooling, employment record, successive addresses, family background, friendships, medical history, financial position, hobbies, leisure interests and beliefs, all serve to single him out from the rest of the population. But to allow the collection of information of that kind under pain of legal penalty for non-disclosure would constitute a substantial intrusion on personal privacy ...

2.5 That privacy interests could give rise to a distinct cause of action was first mooted by New Zealand courts in 1985. In *Tucker v News Media Ownership Ltd*,[8] the applicant sought injunctions preventing News Media Ownership Ltd and others from publishing information about him and certain past offences. The applicant was awaiting a heart transplant and had been the subject of a money-raising campaign in respect of the operation which had received public support. It was argued that, given the state of the applicant's health, publication of the material could lead to stresses that would be potentially lethal to him. Jeffries J said:[9]

> I am aware of the development in other jurisdictions of the tort of invasion of privacy and the facts of this case seem to raise such an issue in a dramatic form. A person who lives an ordinary private life has a right to be left alone and to live the private aspects of his life without being subjected to unwarranted, or undesired, publicity or public disclosure … In my view the right to privacy in the circumstances before the Court may provide the plaintiff with a valid cause of action in this country.

2.6 In later proceedings to rescind or vary the injunctions, McGechan J said:[10]

> I support the introduction into the New Zealand common law of a tort covering invasion of personal privacy at least by public disclosure of private facts … While the American authorities have a degree of foundation upon constitutional provisions not available in New Zealand, the good sense and social desirability of the protective principles enunciated are compelling … Beyond these expressions of support for the concept I will not presently go, although I observe that the need for protection whether through the law of tort or by statute in a day of increasing population pressures and computerised information retrieval systems is becoming more and more pressing. If the tort is accepted as established, its boundaries and exceptions will need much working out on a case by case basis so as to suit the conditions of this country. If the legislature intervenes during the process, so much the better.

7 [1980] 1 NZLR 443, 446 (CA).

8 [1986] 2 NZLR 716.

9 (22 October 1986) HC WN CP 477-86, Jeffries J.

10 [1986] 2 NZLR 716, 733 (HC) McGechan J.

2.7 Momentum for this view gathered. The tort was relied upon for interim injunctions in *Morgan v Television New Zealand*[11] (preventing the broadcast of a documentary about a girl who was the subject of a custody dispute) and *C v Wilson and Horton Ltd*[12] (preventing the defendant from identifying an individual who was being investigated by the Serious Fraud Office).[13] Subsequently, in *Bradley v Wingnut Films Ltd*, Gallen J stated that he was:[14]

> prepared to accept that such a cause of action forms part of the law of this country but I also accept at this stage of its development its extent should be regarded with caution … so that there is a constant need to bear in mind that the rights and concerns of the individual must be balanced against the significance in a free country of freedom of expression.

2.8 On the elements of the tort as they were applied in that case, the application failed. Gallen J considered the elements to be (1) the public disclosure (2) of facts that were private facts, (3) where the matter made public is one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities. The case concerned the publication of a "splatter film" in which one scene depicted a cemetery containing the plaintiff's family tombstone. While the disclosure would be public, the judge considered that the existence of a tombstone in a public cemetery could not be considered a private fact. He also felt the plaintiff would have difficulty establishing that the matter would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.

2.9 Next, in *P v D*,[15] Nicholson J granted an injunction preventing publication of an article that referred to the fact that P, a public figure, had been treated at a psychiatric hospital.[16] Nicholson J said:[17]

> the right of freedom of expression is not an unlimited and unqualified right and in my view is subject to limitations of privacy as well as other limitations such as indecency and defamation. I adopt the statements of Jeffries J, the Court of Appeal and McGechan J in the *News Media Ownership* case and I join with Gallen J in accepting that the tort of breach of privacy forms part of the law of New Zealand.

11 *Morgan v Television New Zealand* (1 March 1990) HC CH CP 67-90, Holland J.

12 (27 May 1992) HC AK CP 765-92, Williams J.

13 Unsuccessful attempts to obtain injunctions based on the tort can be found in: *Re Morgan* (15 March 1990) HC CH CP 93-90, Holland J (injunction was refused because the publication concerned was already in the course of distribution); *Marris v TV3 Network Ltd* (14 October 1991) HC WN CP 754-91, Neazor J (damages were a sufficient remedy for breach of privacy); *Moko-Mead v Independent Newspapers Ltd* (25 October 1991) HC WN CP 813-91, Neazor J; *Hickmott v TVNZ Ltd* (31 March 1993) HC AK CP 213-93, Robertson J (high standard necessary to overcome importance of freedom of expression not reached); *Beckett v TV3* (18 April 2000) HC WHA CP 10-00, Robertson J; *A v Wilson & Horton* (5 May 2000) HC AK CP 7-00 Doogue and Robertson JJ.

14 [1993] 1 NZLR 415, 423 (HC), Gallen J.

15 [2000] 2 NZLR 591 (HC).

16 The Court found that a claim for breach of confidence would not succeed because the information obtained by D (a journalist) could have been received from a person who was not under a duty of confidence, such as a member of the public, and therefore could not be said to have been imparted in circumstances importing an obligation of confidence.

17 [2000] 2 NZLR 591, 599 (HC) Nicholson J.

2.10 As in *Bradley*, the tort was described by reference to the position in the United States. Nicholson J considered that four elements were necessary:[18]

(1) That the disclosure of the private facts must be a public disclosure and not a private one.

(2) Facts disclosed to the public must be private facts and not public ones.

(3) The matter made public must be one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.

(4) The nature and extent of legitimate public interest in having the information disclosed must be weighed.

2.11 The Judge granted the injunction on the basis that the disclosure of the fact of a psychiatric disorder could be considered highly objectionable to a reasonable person, and that there was no legitimate public interest in publication of the information.

2.12 The *P v D* criteria were applied in *L v G*,[19] where damages were awarded for breach of privacy. L was a prostitute and G was her client. G took a number of sexually explicit photographs of L and had one of them published without her consent in an adult magazine. L claimed that the photograph was taken without her consent. Judge Abbott did not consider that the fact that L could not be identified from the photograph was fatal to the action. He considered that the rights protected in a privacy action related not to issues of perception and identification by members of the public but to the loss of the personal "shield of privacy".[20]

Hosking v Runting[21]

2.13 In 2004 the Court of Appeal, by a majority of three to two, held that there is indeed a tort of invasion of privacy in New Zealand. A photographer was commissioned by *New Idea* magazine to photograph the 18-month-old twin daughters of television personality Mike Hosking, following his separation from his wife. Magazines had previously published articles about the Hoskings, touching on a range of personal matters. However, following the birth of their twins, the Hoskings declined further publicity. On learning that the photographs had been taken during a shopping trip and were to be published, the Hoskings sought an injunction restraining the magazine from taking and publishing photographs of the twins, arguing that photographing the children and publishing the photographs without consent amounted to a breach of the twins' privacy.

2.14 In the High Court, Randerson J concluded that New Zealand courts should not recognise a tort that would provide a remedy for the public disclosure of photographs of children taken while they were in a public place, for five broad reasons:[22]

18 [2000] 2 NZLR 591, 599 (HC) Nicholson J.

19 [2002] DCR 234.

20 [2002] DCR 234, 246, Judge Abbott. The Court of Appeal in *Hosking* considered that *L v G* may have been better dealt with as a breach of confidence claim.

21 [2003] 3 NZLR 385 (HC) and [2005] 1 NZLR 1 (CA).

22 [2003] 3 NZLR 385, para 118 (HC) Randerson J.

(1) the deliberate approach to privacy taken by the legislature to date on privacy issues suggested that the courts should be cautious about creating new law in the field;

(2) the tort contended for went well beyond the limited form of the tort recognised in previous decisions and was not supported by principle or authority;

(3) existing remedies were likely to be sufficient to meet most claims to privacy based on the public disclosure of private information and to protect children whose privacy may be infringed;

(4) in the light of subsequent developments,[23] it was difficult to support the privacy cases decided in New Zealand to date; and

(5) to the extent there might have been gaps in privacy law, they should be filled by the legislature, not the Courts.

2.15 The Court of Appeal dismissed the Hoskings' appeal, so it was not strictly necessary for the Court to decide whether there is a right of action for wrongful publication of private information at common law in New Zealand. Nonetheless, a majority of three Judges held that there was such a tort, separate from breach of confidence, but that it did not provide a remedy to the Hoskings to prevent publication of the photographs taken of their children in a public street.[24] The majority gave two judgments: the joint judgment of Gault P and Blanchard J and a separate judgment by Tipping J. Justices Keith and Anderson disagreed that such a tort existed.

2.16 Gault P and Blanchard J considered that two requirements had to be satisfied for the tort to succeed:[25]

> (1) the existence of facts in respect of which there is a reasonable expectation of privacy; and
>
> (2) publicity given to those private facts that would be considered highly offensive to an objective reasonable person.

2.17 They also said that there is "a defence enabling publication to be justified by a legitimate public concern in the information". The burden for proving the defence is on the defendant, and it is not available where the matter is of no more than general interest or titillation, or gives rise to curiosity.

2.18 In finding the existence of the tort, Gault P and Blanchard J noted that the legislative landscape is important. They noted the omission of a right to privacy in the New Zealand Bill of Rights Act 1990 (BORA)[26] and the range of protections contained in the Privacy Act 1993, Broadcasting Act 1989 and Harassment Act 1997 (see below). They concluded that such legislative protection cannot be regarded as so comprehensive as to preclude common law remedies.

---

23 By which he, presumably, meant the lack of satisfactory development of an invasion of privacy tort in other jurisdictions, apart from the United States.

24 See also *Murray v Express Newspapers plc* [2007] EWHC 1908 (concerning a photograph taken in the street that included a child of author JK Rowling).

25 *Hosking v Runting* [2005] 1 NZLR 1, para 117 (CA) Gault P and Blanchard J.

26 See paras 2.60-2.73 below.

A "reasonable expectation of privacy"

2.19 To Gault P and Blanchard J, facts meeting the first criterion are "private facts": known to some people, but not to the world at large. There is no simple test as to what is a private fact. In the context of *Hosking*, they noted that the right to privacy is not automatically lost when a person is a public figure, but his or her reasonable expectation of privacy in relation to many areas of life will be correspondingly reduced. While the special position of children is not to be lost sight of, they also considered that there is inevitably some reduction in the privacy of the families of public figures.[27]

2.20 Tipping J considered that a reasonable expectation of privacy could arise from the nature of the information or material, or the circumstances in which the defendant came into possession of it, or both.

"Publicity"

2.21 The judgments do not provide a great deal of insight as to what amounts to sufficient "publicity" for the tort to be established. However, Gault P and Blanchard J suggested that publicity had to be "widespread".[28]

Publicity that is highly offensive

2.22 Gault P and Blanchard J considered it was quite unrealistic to contemplate legal liability for all publications of private information. The tort should therefore relate only to publicity that was truly humiliating and distressful or otherwise harmful to the individual concerned. The test related to *the publicity*, not to whether the information was private.

2.23 While Tipping J agreed with the existence of the tort, he formulated the test differently as it relates to this aspect. He considered that this criterion of Gault P and Blanchard J's test was implicit in the first. Thus, for Tipping J the first and fundamental ingredient of the tort was that the claimant must "be able to show a reasonable expectation of privacy in respect of the information or material which the defendant has published or wishes to publish". Such an expectation could "arise from the nature of the information or material or the circumstances in which the defendant came into possession of it", and part of establishing that ingredient was whether the breach would cause a reasonable person "substantial" offence and harm. Tipping J's formulation therefore set a lower threshold for harm than the other majority judgment.

2.24 The majority judgments agreed, however, that offensiveness was to be determined by reference to an objective reasonable person.

Legitimate public concern

2.25 Both majority judgments construed the "legitimate public concern" element as a defence to the action with the burden on the defendant, rather than part of the tort itself, as had been held in *P v D*. As a defence, it would ensure that the scope

27 Compare the conclusions of the English Court of Appeal in *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, para 46.

28 *Hosking v Runting* [2005] 1 NZLR 1, para 125, Gault P and Blanchard J.

of privacy protection would not exceed such limits on the freedom of expression as were justified in a free and democratic society. The importance of the value of freedom of expression would therefore be related to the extent of legitimate public concern in the information.

2.26 Gault P and Blanchard J emphasised the use of the term "concern" to distinguish between matters of general interest and curiosity to the public and matters which were of legitimate public concern.

Remedies

2.27 The main redress for the action is damages, and Gault P and Blanchard J considered that injunctive relief may be granted only in appropriate cases. They noted the defendant's concern that a less stringent approach would be taken to interim restraint in privacy than in defamation cases. They concluded that an injunction to restrain publication in the face of an alleged interference with privacy would usually only be available where there was "compelling evidence of most highly offensive intended publicising of private information and there was little legitimate public concern in the information".[29]

2.28 Tipping J agreed that the primary remedy would be damages. He considered that:[30]

> Prior restraint by injunction … will be possible but should, in my view, be confined to cases which are both severe in likely effect and clear in likely outcome. Freedom of expression values will ordinarily prevail at the interlocutory stage. I am mindful of the chilling effect which potential claims for damages for invasion of privacy might have on the activities of news media organisations and perhaps others. But against that I am mindful too of the considerable distress which unwarranted invasion of privacy can cause. The right to freedom of expression is sometimes cynically invoked in aid of commercial advantage. Of course the right to freedom of expression exists in the commercial field, but it should not be allowed to become a justification for what may be little more than a desire to boost circulation or ratings …

Dissenting judgments

2.29 Keith and Anderson JJ wrote separate judgments denying the existence of the tort in New Zealand. In support of his argument, Keith J cited:[31]

> the central role in our society of the right to freedom of expression; the array of protections of relevant privacy interests in our law against disclosures of private information and the deliberate and specific way in which they are in general elaborated; and the lack of an established need for the proposed cause of action.

2.30 He also noted Parliament's express exclusion of the news media in its news-gathering capacity from the scope of general privacy legislation. Furthermore, he considered that:[32]

29 *Hosking v Runting* [2005] 1 NZLR 1, para 158, Gault P and Blanchard J.

30 *Hosking v Runting* [2005] 1 NZLR 1, para 258, Tipping J.

31 *Hosking v Runting* [2005] 1 NZLR 1, para 177, Keith J.

32 *Hosking v Runting* [2005] 1 NZLR 1, para 220, Keith J.

> [t]o the argument that because the general tort is rarely invoked there is no harm in recognising it, there are two answers: that limited effect demonstrates a lack of pressing need … a need which, especially in terms of s 5 of the Bill of Rights, has to be demonstrably justified by the proponents; and the very existence of an ill-defined tort carries with it costs, not simply financial but also those arising from the chilling effect it may have on freedom of expression.

2.31 Anderson J also criticised the imprecise nature of the new tort, "both semantically and in terms of its application in reality".[33] He concluded:

> In my respectful view, this new liability, created in a side wind, is amorphous, unnecessary, a disproportionate response to rare, almost hypothetical circumstances and falls manifestly short of justifying its limitation on the right to freedom of expression affirmed by the NZBORA.

Developments since *Hosking*

2.32 There has not been a great deal of case law on the privacy tort since *Hosking*, but as John Burrows has noted, the cases show the potential breadth of privacy claims.[34]

2.33 Injunctions have been granted in a few instances. Examples include an injunction in favour of ex-National Party leader Don Brash in relation to emails copied from his computer system without his authority or knowledge.[35] Another case involved an interim injunction, granted to a descendant of a notorious New Zealand murderer. The descendant wanted to keep his identity, and his relationship to the murderer, private. The injunction has not been challenged and still stands. The case does not appear to be recorded anywhere.

Brown v Attorney-General[36]

2.34 In *Brown*, the plaintiff had recently been released on parole after serving three-and-a-half years of a five-year sentence for the kidnapping and indecent assault of a five-year-old boy. Local police arrived at the plaintiff's residence and took photographs of him. The photographs were taken with the plaintiff's consent, but he believed they were for police records only. Subsequently, the police circulated a flyer in the area which included one of the photographs, warned locals that the plaintiff was a convicted paedophile living in their area, and encouraged residents to be aware of the plaintiff and his activities. The flyer did not reveal his exact address, but named his street. The existence of the flyer was subsequently widely reported in the media.

2.35 As a result, the plaintiff received verbal abuse when he went out in public, was physically assaulted on two separate occasions and received hate mail. As a consequence, he rarely left his apartment. The plaintiff became recognisable

33 *Hosking v Runting* [2005] 1 NZLR 1, para 270, Anderson J.

34 John Burrows "Invasion of Privacy – Hosking and Beyond" [2006] NZ Law Rev 389, 403.

35 *Brash v Doe* (16 November 2006) HC WN CIV 2006-485-2605, MacKenzie J. This injunction was lifted some days later.

36 NZAR [2006] 552 (DC) Judge RLB Spear.

in the wider Wellington area and continued to be the victim of harassment after he moved. He successfully sued the Attorney-General for damages for invasion of privacy.

2.36 Judge Spear was not concerned by the different expressions of the tort in *Hosking*, and considered that the outcome would be the same no matter which approach was adopted. On the question of whether a reasonable expectation of privacy arose, the Judge considered that the content of the flyer as a whole and the overall effect of its message should be considered and that the test is not whether a convicted paedophile would have a reasonable expectation of privacy but whether an objective observer would hold such a view.

2.37 He acknowledged that the flyer revealed nothing about the plaintiff that was not in the public domain except that he had moved to the area and had just been released from prison. However, he accepted that a photograph could amount to information in which there might be a reasonable expectation of privacy. Looking at the flyer as a whole, he concluded that the inclusion of the photograph meant that "any hope that the Plaintiff could live privately was dashed". The plaintiff could reasonably expect that "his likeness and general address would not be published in such a sensational way". The context in which the photograph was taken was also relevant and the plaintiff could have a reasonable expectation that the photograph would only be used for legitimate Police business. Judge Spear considered that the Police should have obtained the express consent of the plaintiff. The Judge also found that the publicity given to the information would be considered highly offensive to an objective person standing in the shoes of the plaintiff.

2.38 Although the Attorney-General argued that the defence of legitimate public concern applied and justified the publication, there was expert evidence that "public shaming" such as had resulted from the flyer was more likely to increase the risk to the community than lessen it. The Judge characterised the defence as requiring "a pressing need in the public interest".[37] He concluded that the nature of the flyer and information contained in it, and the predictable vigilante response, meant that publication of the material could not be considered of legitimate public concern. Damages of $25,000 were awarded.

2.39 The case is notable since, unlike *Hosking*, it did not involve a question of publication by the media. Further, the Judge had particular problems in the application of the requirement that the publicity had to be highly offensive to an objective reasonable person in the shoes of the complainant. Judge Spear said "The test of course is not for the objective reasonable paedophile but of a reasonable person in the shoes of the person that the publication is about".[38] As Burrows notes, the test is extraordinarily difficult to apply where the subject of the publication is not an "ordinary" person.[39]

37 Although he noted that this could leave the threshold of the defence too high.

38 NZAR [2006] 552, para 81 (DC) Judge RLB Spear.

39 John Burrows "Invasion of Privacy – Hosking and Beyond" [2006] NZ Law Rev 389, 405–406.

Andrews v Television NZ Ltd[40]

2.40 *Andrews* concerned an unsuccessful claim for damages by a husband and wife who were involved in a car crash. TVNZ had filmed the efforts of firefighters to free the applicants from their damaged car as part of a series which portrayed the lives and daily work of fire officers. The applicants did not know that they had been filmed and were not informed before the tapes were broadcast, a year after the accident. The programme depicted the applicants injured in the car and viewers could hear a distressed conversation in which the wife expressed her love and concern for her husband. While her face was pixelated, Allan J considered that the pixelation was not always sufficient to obscure the whole of her face. The plaintiffs were greatly distressed by the screening of the programme and sued for damages of $100,000 for breach of their privacy.

2.41 Allan J applied the *Hosking* criteria in turn. He considered that while the event took place in public, the nature of the intimate and personal conversations between the husband and wife, combined with the fact that the footage went beyond mere observation of the scene, did give rise to a reasonable expectation of privacy. The Judge considered that the morality and behaviour of a plaintiff could be a relevant factor as to whether a reasonable expectation of privacy existed, but that it was difficult and undesirable to lay down any general principle governing the extent to which personal culpability was relevant.[41] The plaintiffs in *Andrews* were both found to be over the legal alcohol limit when the accident occurred. However, the Judge considered that on the surrounding facts of the case, the plaintiffs did not deserve to lose their right to privacy because they may have been the authors of their own misfortune.

2.42 Allan J went on to consider whether, if there were private facts, publication of them would be "highly offensive to the reasonable person in the shoes of the complainant". He considered that the burden was a high one, and that the mind that must be considered is the person who is affected by the publicity, assuming that person to be a reasonable person of ordinary sensibilities. If the plaintiff was not of ordinary sensibilities, the court should consider the mind of a fictitious "reasonable person". Finally, he considered that the disclosure of relatively inoffensive facts could become offensive by the extent and tone of a publication. The manner of disclosure is therefore relevant.

2.43 On the facts, the Judge did not consider that reasonable people in the Andrews' shoes would find the publication to be highly offensive. First, there was nothing that showed the husband in a bad light or that he considered humiliating or embarrassing. Similarly, there was nothing that the wife could identify that she claimed to be offensive, humiliating or embarrassing. Allan J noted that this did not necessarily lead to a conclusion that nothing about the disclosure was humiliating or distressful, but he considered that the Andrews' annoyance

40 (15 December 2006) HC AK CIV 2004-404-3536, Allan J.

41 Referring to *Australian Broadcasting Corporation Ltd v Lenah Game Meats* (2001) 208 CLR 199 (HCA); *Campbell v MGN* [2004] 2 AC 457, para 24 (HL) and *Theakston v MGN Ltd* [2002] EMLR 22.

was in fact aimed at the lack of notice that they were being filmed for subsequent broadcast. He concluded that a failure to obtain consent was not an ingredient of the tort of breach of privacy.[42]

2.44 Allan J also considered whether identification was required to establish the tort. Whereas the Broadcasting Standards Authority requires that a complainant be able to establish that he or she is identifiable beyond his or her immediate circle before a privacy complaint can be upheld,[43] the Judge considered that:[44]

> In cases such as the present, it seems that plaintiffs will ordinarily be concerned about being identified in the context of the facts of a particular case to those who know them but do not know the facts. Identification to those who already know the facts will, in general, be of little moment. Identification to the world at large, which does not know the plaintiff, will often likewise be of limited concern although cases will no doubt arise in which a plaintiff becomes known to the world at large simply by reason of the publicity. But publication to those who know the plaintiff, but not the facts, is likely in many instances to be central to a plaintiff's claim.

2.45 He considered that the broadcast could have identified the Andrews to people who knew them but were not aware of the accident or its circumstances.

2.46 Finally, Allan J considered the defence of legitimate public concern. The extent of the invasion of privacy was relevant: the Judge would have upheld the defence because the programme had a serious underlying purpose and because, had he found an invasion of privacy, it would have fallen towards the lower end of the scale. In assessing the defence, Allan J noted that the courts were to balance the interests of the parties and that usually this would require balancing privacy with freedom of expression. He also considered that while the matter had to be properly within the public interest, not just of general interest, the court would allow a degree of journalistic latitude so as to avoid robbing a story of its attendant detail.

2.47 Again, *Andrews* raises a number of questions about factors that are relevant to establishing the elements of the tort. In particular, is a plaintiff's behaviour relevant to whether he or she can mount a successful claim under the action; and is it necessarily the case that the private facts should tend to show a person in bad light for them to be offensive, humiliating or embarrassing?

Television New Zealand Ltd v Rogers[45]

2.48 In *Rogers*, a man called Lloyd had been imprisoned for the manslaughter of a woman in 1994. His conviction was quashed in 2004 and Rogers was charged with the woman's murder. While he was in custody, and without counsel present, the police took Rogers to the property where the murder had taken place

42 Consent and notification issues do fall within the jurisdiction of the Broadcasting Standards Authority, but no complaint was made to that body.

43 See, for example, *TVNZ Ltd v BA* (13 December 2004) HC WN CIV 2004-485-1299, Miller J.

44 *Andrews v TVNZ* (15 December 2006) HC AK CIV 2004-404-3536, para 60 Allan J.

45 [2008] 2 NZLR 277 (SC).

and a videoed reconstruction took place in which Rogers confessed to the killing. The video was ruled inadmissible at his trial and Rogers was subsequently acquitted.

2.49 A copy of the video had been given by the police to TVNZ. After the trial, Rogers became aware that TVNZ intended to broadcast the video. In the High Court, Justices Venning and Winkelmann granted a permanent injunction[46] against broadcast on the basis that once the tape was ruled inadmissible as evidence at trial, Rogers had a reasonable expectation that its contents would remain private. They also considered that the context of the proposed broadcast would be highly offensive to a reasonable person because its purpose would be to question whether the jury might have reached a different view had they seen the video. After weighing the interests of freedom of expression and open justice with Rogers' interests, the Judges considered that the defence of legitimate public interest was not open to TVNZ.

2.50 The Court of Appeal unanimously allowed the appeal and set aside the orders made against TVNZ.[47] O'Regan and Panckhurst JJ found that, while the facts did establish an invasion of privacy, the public interest defence was available to TVNZ. The defence was essentially a matter of proportionality and the privacy value of the facts concerned was at the low end of the scale. It followed that the degree of legitimate public concern necessary to establish the defence was also low. They considered that cases of prior restraint on the basis of an allegation of invasion of privacy should be rare, given their potentially chilling effect on freedom of expression.

2.51 In a separate judgment, William Young P doubted that what was shown on the videotape was of a sufficiently private or personal character to found a legal claim for interference with privacy. He also agreed with the majority that the defence of legitimate public concern applied in the circumstances.

2.52 The Supreme Court's decision on appeal did little to clarify the boundaries of the tort. The judges decided 3:2 to allow the broadcast. The Chief Justice criticised the process followed in the case, which had proceeded without pleadings. Accordingly, she would have remitted the case to the High Court and granted an interlocutory injunction in the interim. While she appeared to accept the existence of a tort of invasion of privacy as stated by the Court of Appeal in *Hosking*, she noted that its limits are not clearly settled. She also considered that developments in other jurisdictions since *Hosking* mean that it is necessary to be cautious. In particular, citing *Campbell v MGN Ltd*,[48] she queried whether the tort required that publicity should be "highly offensive". She also stated that *Hosking* "did not purport to answer all questions about liability where privacy interests are adversely affected".

46 (2005) 22 CRNZ 668 (HC).

47 [2007] 1 NZLR 156 (CA).

48 [2004] 2 AC 457, paras 94–96 Lord Hope and para 22 Lord Nicholls.

2.53 Anderson J, who had dissented in *Hosking*, agreed with the Chief Justice's conclusion, but went further in stating that *Hosking* "was decided by a bare majority and both the existence of the tort and the scope of it, if it continues to be recognised, will fall to be reviewed by this Court in an appropriate case."[49]

2.54 The majority of the Supreme Court determined that the broadcast should go ahead. On the question of privacy, they each applied the *Hosking* tort but determined that there could be no expectation of privacy in the video since Rogers must have known that the video was being recorded for use as police evidence in the trial and that it was intended that it would be shown to a jury in a public courtroom.

2.55 Two main issues arise from the Supreme Court judgments. First, there were differing views on when a reasonable expectation of privacy needs to arise. The majority judges considered that it was at the time the video was made.[50] However, the Court of Appeal had considered that the expectation arose at the time when the video was ruled inadmissible. It was thus able to find that a reasonable expectation of privacy did exist in the case. In contrast, the Chief Justice cited overseas authority that suggests the expectation of privacy arises at the time of publication.[51]

2.56 Secondly, there is continuing disagreement about the threshold for injunctions to be granted in privacy cases. Tipping J noted the approach in defamation cases: that a defendant who undertakes to prove the truth of the allegation will not be made the subject of prior restraint by interim injunction unless the case for justification could not possibly succeed. He stated that that approach "has been carefully worked out so as not to encroach in advance on rights to freedom of expression. The position is broadly analogous in relation to the tort of invasion of privacy."[52] The Chief Justice, however, suggested that claims for privacy differed from claims for defamation, where reputation can be restored. Thus, injunctions may be granted more readily in privacy cases. She considered that:[53]

> The analogy with interlocutory restraint in defamation proceedings is imperfect and needs to be treated with caution. Injunctive relief may well be appropriate. Whether freedom of information considerations should prevail depends on the circumstances of the particular case and all interests properly engaged.

2.57 Finally, there was some recognition of the fact that while the video essentially contained public facts, such a video could still give rise to a reasonable expectation of privacy because of the "enhancement" given to the material by showing the material "live" and because of the extent to which it displayed an individual's demeanour.[54]

---

49 *Television New Zealand v Rogers* [2008] 2 NZLR 277, para 144 Anderson J.

50 *Television New Zealand v Rogers* [2008] 2 NZLR 277, para 48 Blanchard J, para 63 Tipping J and paras 104–105 McGrath J.

51 *Television New Zealand v Rogers* [2008] 2 NZLR 277, para 26, citing *Vickery v Nova Scotia* (Prothonotary of the Supreme Court) [1991] 1 SCR 671 (Can SC) and *R v Chief Constable of the North Wales Police, ex p AB* [1997] 4 All ER 691.

52 *Television New Zealand v Rogers* [2008] 2 NZLR 277, para 66 Tipping J.

53 *Television New Zealand v Rogers* [2008] 2 NZLR 277, para 38 Elias CJ.

54 *Television New Zealand v Rogers* [2008] 2 NZLR 277, para 68 Tipping J, para 100 McGrath J.

Mafart & Prieur v Television New Zealand Ltd[55]

2.58 It is worth noting that the courts may be increasingly willing to consider aspects of privacy that fall outside the parameters of the *Hosking* tort. *Mafart* related to an application by TVNZ to search court records with the aim of obtaining and broadcasting a videotape of committal proceedings in which two French secret agents pleaded guilty to a charge of manslaughter for their part in blowing up the *Rainbow Warrior* in Auckland Harbour in 1985. In the Court of Appeal, Hammond J stated that:[56]

> It is a common and lamentable part of entering the public gaze that the media tends to promote one salient feature of an incident (often glorified as a 30-second sound byte), with unfortunate and unfair results. Not the least is a refusal (or at least a misportrayal) which fails to respect the fact that people may well be different in private than in public. We mention these sort of factors out of fairness for the appellants, and because we are aware of the compelling impact of scorn, hate and disgust that unwise or unthinking media exposure can have for individuals. … Hence, if there was any evidence that what was being resorted to by TVNZ was something designed to humiliate, or even if it might have had that effect in relation to the appellants, then that would be a matter for grave concern. But … in this instance the appellants seem not to have been afflicted by any concerns of that kind. There is no evidence at all of any kind of intrusion here of a humiliating variety.

2.59 Cheer suggests that, here, the Court appeared prepared to contemplate the existence of a "false light" privacy claim.[57]

Privacy and the New Zealand Bill of Rights Act 1990 (BORA)[58]

2.60 The long title to the New Zealand Bill of Rights Act 1990 states that it is "an Act to affirm New Zealand's commitment to the International Covenant on Civil and Political Rights" (ICCPR). Article 17 of the ICCPR provides a right to privacy:

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

Furthermore, article 2 of the ICCPR obliges states parties to ensure that those whose rights are violated have an effective remedy. However, BORA does not include a statement of the general right to privacy recognised in the ICCPR.

55 [2006] 3 NZLR 534 (CA).

56 [2006] 3 NZLR 534, paras 62-63 (CA).

57 Ursula Cheer "The Future of Privacy: Recent Legal Developments in New Zealand" (2007) Canta LR 169, 198. The United States tort of "false light" invasion of privacy is discussed in chapter 4.

58 See also discussion in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 90-97.

2.61 The White Paper on the proposed Bill of Rights stated that the Government was not, at the time, inclined to "entrench" a vague and uncertain privacy right in the New Zealand climate. The commentary on the Bill stated that:[59]

> There is not in New Zealand any general right to privacy although specific rules of law and legislation protect some aspects of privacy. It would be inappropriate therefore to attempt to entrench a right that is not by any means fully recognised now, which is in the course of development, and whose boundaries would be uncertain and contentious.

2.62 The exclusion of the right was the subject of debate and these reasons were not accepted by all commentators.[60] The existence of the Privacy Act 1993, the continuing privacy jurisprudence of the Broadcasting Standards Authority and the development of the privacy tort, mean that the context today is somewhat different from that in which the Bill of Rights was developed.

2.63 Privacy interests are, however, directly protected by section 21 of BORA ("right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise") and other provisions go to protect rights that might be said to represent elements of a person's private life and autonomy. These include the right to freedom of thought, conscience, and religion, the right to freedom of association and the right to freely manifest religion and belief. Bodily privacy is protected to some extent by the rights not to undergo medical experimentation without consent and to refuse medical treatment. However, the omission of a distinct privacy right means that BORA differs from some other human rights documents, for example, the European Convention on Human Rights which is now part of United Kingdom law and which contains the right to respect for a person's private and family life, home and correspondence.[61] This leads to differences in approach: in Europe, privacy and other rights such as freedom of expression have equal status and must be balanced against each other if there is a conflict between them. In New Zealand, the fact that privacy is not included in BORA has meant that it has sometimes tended to be treated as of different status than rights affirmed in BORA.

2.64 Under section 28, an existing right or freedom is not abrogated or restricted because it is not included or not fully included in BORA. Thus, the omission of the right to privacy does not mean that it carries no weight. Furthermore, New Zealand remains obligated at international law to protect citizens' right to privacy and to ensure an effective remedy for its breach. It follows that a question still arises as to whether and how the protection of privacy as contemplated by the tort is to be balanced against the rights contained in BORA, and specifically

---

59 *A Bill of Rights for New Zealand: A White Paper* (Department of Justice, Wellington, 1985) para 10.144.

60 See, in particular, Jerome Elkind and Antony Shaw *A Standard for Justice: a Critical Commentary on the Proposed Bill of Rights for New Zealand* (Oxford University Press, Auckland, 1986) 118-123; Blair Stewart "Should the Right to Privacy be Expressly Recognised in the New Zealand Bill of Rights Act?" (Paper prepared for Privacy Issues Forum, University of Auckland, 12 May 1994).

61 See chapter 4 below. A right to privacy is also expressly mentioned in the Charter of Human Rights and Responsibilities Act 2006 (Vic) and the Human Rights Act 2004 (ACT). However, neither the United States Constitution nor the Canadian Charter of Rights and Freedoms recognise an explicit right to privacy.

the right to freedom of expression contained in section 14: "Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form."

2.65 Is BORA relevant in relations between private individuals (such as in *Hosking*), and, if so, how determinative should the BORA rights be? Notwithstanding that, under section 3, the Act does not apply directly to acts done by private persons,[62] the court in *Hosking* considered that BORA was relevant both to the creation of the new tort and to its application in individual cases. Gault P and Blanchard J characterised the starting point as being that:[63]

> [w]hile developments in the common law must be consistent with the rights and freedoms contained in the Bill of Rights Act, such developments are not precluded merely because they might encroach upon those rights and freedoms. It becomes a matter of whether such common law encroachment meets the test of a reasonable limit on the applicable right or freedom which is demonstrably justified in a democratic society in s 5.

Tipping J also considered that "it will often be appropriate for the values which are recognised in [the BORA] context to inform the development of the common law in its function of regulating relationships between citizen and citizen."[64]

2.66 The dissenting judgments placed significant emphasis on section 14 as the basis for refusing to recognise the tort. However, the position of the majority is that the tort represents a justifiable encroachment on the right to freedom of expression.

2.67 BORA is also relevant because it forms part of the determinative process to be carried out in each case. The balancing required between the tort and freedom of expression forms part of the rationale for the defence of legitimate public concern itself.[65] It also forms part of the balancing exercise required in assessing that defence in each case.[66]

2.68 While not necessarily suggesting that the court was wrong to apply BORA when deciding whether to create the tort, Andrew Geddis has commented that the reasoning in the *Hosking* judgments as to why the Act should apply in purely private disputes is unsatisfactory.[67] Geddis has further argued that clarification is required with regard to the respective weight to be given to the right to freedom of expression, as recognised by BORA, and the right to privacy not recognised in BORA but given effect through the tort. He suggests that: "while the affirmed rights are accepted as being relevant to the judicial decision, they are not then

62 Section 3 provides: "This Bill of Rights applies only to acts done—(a) By the legislative, executive, or judicial branches of the government of New Zealand; or (b) By any person or body in the performance of any public function, power, or duty conferred or imposed on that person or body by or pursuant to law."

63 *Hosking v Runting* [2005] 1 NZLR 1, para 111 (CA).

64 *Hosking v Runting* [2005] 1 NZLR 1, para 229 (CA).

65 *Hosking v Runting* [2005] 1 NZLR 1, para 130 Gault P and Blanchard J: "Furthermore, the scope of privacy protection should not exceed such limits on the freedom of expression as is justified in a free and democratic society. A defence of legitimate public concern will ensure this."

66 *Hosking v Runting* [2005] 1 NZLR 1, para 132 Gault P and Blanchard J: "The importance of the value of the freedom of expression therefore will be related to the extent of legitimate public concern in the information publicised."

67 Andrew Geddis "The Horizontal Effects of the New Zealand Bill of Rights Act, as Applied in Hosking v Runting" [2004] NZ Law Rev 681.

accorded any particular weight vis-à-vis other relevant factors by virtue of their inclusion in [BORA]".[68] When similarly commenting on the weight to be accorded to privacy, Thomas J noted in *Brooker v Police* that Gault P and Blanchard J arrived at their decision without negating the notion that privacy may be a right or asserting that it is to be treated as a "value".[69]

2.69 The respective weight to be given to the two rights or interests has been the subject of ongoing judicial debate.[70] For example, in *Brooker*, the Supreme Court considered whether a protest unduly impacted on the spatial privacy of the policewoman at whom the protest was directed and whether privacy was therefore a justifiable limitation on the protester's freedom of expression.[71] The appeal concerned the meaning of "behaves in [a] disorderly manner" under section 4(1)(a) of the Summary Offences Act 1981. The Supreme Court was divided 3:2.

2.70 The majority overturned the decision of the Court of Appeal and found that the privacy intrusion did not justify a limitation on freedom of expression. In one of the majority judgments, Elias CJ commented:[72]

> I have misgivings about whether it is open to the courts (which are bound by s 3 of the New Zealand Bill of Rights Act) to adjust the rights enacted by Parliament by balancing them against values not contained in the New Zealand Bill of Rights Act, such as privacy, unless the particular enactment being applied unmistakeably identifies the value as relevant.

2.71 In the first dissenting judgment, however, McGrath J regarded the interest of New Zealand citizens to be free from intrusions in their home environment as a value that, in the abstract, is close to being as compelling as freedom of speech,[73] and considered that it was necessary to balance the conflicting rights.

2.72 In the second dissenting judgment, Thomas J asserted that both freedom of expression and privacy should be recognised as fundamental values and accorded neither presumptive nor paramount status but weighed one against the other in a manner designed to afford the greatest protection to both:[74]

> I favour regarding privacy as an existing right which has not been abrogated or restricted by reason only that it has not been expressly referred to in the New Zealand Bill of Rights Act 1990. At the very least, I believe that it should be regarded as a "fundamental value." As privacy has not yet been judicially accorded the status of a right, however, I proceed on the basis that what is to be evaluated is the fundamental value underlying the right to freedom of expression against the fundamental value of privacy. Two fundamental values compete for ascendancy.

---

68 Andrew Geddis "The Horizontal Effects of the New Zealand Bill of Rights Act, as Applied in Hosking v Runting" [2004] NZ Law Rev 681, 700.

69 *Brooker v Police* [2007] 3 NZLR 91, para 213, fn 181.

70 See New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP 19, Wellington, 2008) 90–95.

71 Although the protest took place on a public road and did not disturb the public at large, the constable's house was only 3 metres from the road, she was awoken (after working a night shift) by knocking on her door and the protest was directed against her personally in her home.

72 *Brooker v Police* [2007] 3 NZLR 91, para 40 Elias CJ.

73 *Brooker v Police* [2007] 3 NZLR 91, para 129 McGrath J.

74 *Brooker v Police* [2007] 3 NZLR 91, para 164 Thomas J.

2.73 Ultimately, as Ursula Cheer has noted, a more principled approach would be desirable:[75]

> In privacy cases the process should not be an amorphous, fact-specific approach to legitimate public concern, but one that tests the value of privacy both descriptively and normatively, and contrasts it with the right to freedom of expression.

Other civil remedies

2.74 Other civil remedies may be called upon to provide protection to privacy concerns. Some of the remedies are frequently pleaded in the alternative in privacy actions and while their protection of privacy interests may be limited, they overlap with or protect elements of privacy not captured by the *Hosking* tort.

Breach of confidence

2.75 The action of breach of confidence protects values which are similar to privacy, and has formed the foundation of the direct protection of privacy in England.[76]

2.76 Stephen Todd notes that there has been debate about the jurisdictional basis of breach of confidence. Courts have been willing to found actions on express or implied terms in contractual relationships, on equitable principles, by analogy with intellectual property rights such as patents, and by reference to an independent tort in its own right.[77]

2.77 The three elements of the action are:[78]

(1) The information itself must have the necessary quality of confidence about it.

(2) The information must have been communicated in circumstances importing an obligation of confidence.

(3) Unauthorised use of that information must have been made, or be about to be made, to the detriment of the person communicating it.

2.78 In New Zealand, the action will protect privacy interests only so long as these criteria are met, and it is primarily the second factor which limits the action's efficacy for privacy claims.

2.79 In England, the courts have found that an obligation of confidence can arise in circumstances where it is obvious that information was confidential, even if it was not communicated in the course of a confidential relationship.[79]

---

75 Ursula Cheer "The Future of Privacy: Recent Legal Developments in New Zealand" (2007) Canta LR 169, 189.

76 Courts in the United Kingdom have so far declined to treat invasion of privacy as a cause of action in itself. See chapter 4.

77 Stephen Todd "Interference with Intellectual Property" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 575, 611-612.

78 See *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 47–48.

79 See chapter 4 below. See also, for example, *Attorney-General v Guardian Newspapers (No 2)* [1990] 1 AC 109, 281 (HL) Lord Goff (the "Spycatcher" decision). See further Nicole Moreham "Douglas and others v Hello! Ltd – the Protection of Privacy in English Private Law" (2001) 64 MLR 767; Gault P and Blanchard J in *Hosking v Runting* [2005] 1 NZLR 1, paras 23–53.

In the leading case of *Campbell v MGN*,[80] the House of Lords allowed a well-known celebrity model damages when a newspaper published details of drug therapy she was undergoing, together with a photograph of her outside a rehabilitation centre.[81] While the case proceeded on the ground of breach of confidence, the term "privacy" occurs many times in the judgment.[82] Lord Nicholls noted the artificiality of the "confidence" label and that it might be more transparent to acknowledge that what is really being talked about is invasion of privacy. He said:[83]

> The continuing use of the phrase "duty of confidence" and the description of the information as confidential, is not altogether comfortable. Information about an individual's private life would not in ordinary usage be called confidential. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information.

The boundaries of the breach of confidence action in England have been further expanded under the influence of the Human Rights Act 1998 (UK).[84]

2.80 New Zealand courts have refused to interpret the second factor so broadly, on the grounds that to do so would affect the basis of breach of confidence actions themselves:[85]

> If breach of confidence is to be used as the privacy remedy in New Zealand, then the requirement of a confidential relationship must necessarily change. That will lead to confusion in the trade secrets and employment fields.

2.81 Nevertheless, provided that disclosed private information was communicated in circumstances importing an obligation of confidence, the action may provide protection to privacy interests in New Zealand.

Defamation

2.82 A defamation action will lie in respect of the publication of information (including photographs) about the plaintiff that may bring him or her into hatred, ridicule or contempt.[86] Defamation actions are directed at the vindication of a person's reputation, and at providing compensation for the injury to reputation, for the natural injury to feelings, and for the grief and distress caused.[87]

---

80 *Campbell v MGN* [2004] 2 AC 457 (HL).

81 Campbell accepted that the newspaper was entitled to disclose that she was a drug addict and was receiving treatment for her addiction (given her previous public statement that she was not a drug addict) but she objected to the publication of details of her treatment and photographs of her leaving Narcotics Anonymous meetings that made the location identifiable.

82 John Burrows "Invasion of Privacy – Hosking and Beyond" [2006] NZ Law Rev 389, 390.

83 *Campbell v MGN* [2004] 2 AC 457, 465 (HL). See further as to the similarity between the breach of confidence doctrine and the privacy tort: Andrew Geddis "*Hosking v Runting*: A Privacy Tort for New Zealand" (2005) 13 Tort L Rev 5, 7; *Wainwright v Home Office* [2004] 2 AC 406, 422 (HL) Lord Hoffmann (quoting Sedley LJ in *Douglas v Hello! Ltd* [2001] QB 967, 1001).

84 See *Douglas and others v Hello! Ltd* [2005] EWCA Civ 595, [2006] QB 125 and *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446. For further discussion see chapter 4.

85 *Hosking v Runting* [2005] 1 NZLR 1, para 49 (CA) Gault P and Blanchard J.

86 *Parmiter v Coupland* (1840) 6 M & W 105, 108; 151 ER 340.

87 *Television New Zealand Ltd v Keith* [1994] 2 NZLR 84, 86 (CA).

A defamation action can only therefore be relied upon to protect privacy interests so far as it concerns publication of private information that lowers reputation. It is here that the privacy action and defamation differ.

2.83 An example of a situation in which the action could protect privacy interests arose in *Ettingshausen v Australian Consolidated Press Ltd*.[88] The New South Wales Supreme Court held that a published photograph of a well-known sportsman naked in the shower was capable of subjecting him to a more than trivial degree of ridicule and therefore was capable of defaming him.

2.84 It is a defence to a defamation action that the information published is true in substance and in fact.[89] Again, this limits its utility for privacy actions since they are usually motivated by a desire to protect truthful private information.

2.85 Defamation proceedings are also subject to the defence of honest opinion.[90] Thus, any individual has the right to comment on a matter of public interest so long as their opinion is honestly held and the speaker has his or her basic facts right. However, the defence applies only to mere expressions of opinion and not to assertions of fact.

2.86 No proceedings lie in respect of defamation of a dead person. However, a corporate body may maintain proceedings for defamation in the same way as an individual, provided the imputation reflects upon the company or corporation itself and not merely upon its members or officials,[91] and provided the publication has caused it, or is likely to cause it, pecuniary loss.[92]

Nuisance

2.87 A private nuisance is an unreasonable interference with a person's right to the use or enjoyment of an interest in land. The action has been used overseas to protect privacy interests, but there is no New Zealand case law to this effect. In *Baron Bernstein of Leigh v Skyviews & General Ltd*, while the plaintiff's action did not succeed, Griffiths J said:[93]

> The present action is not founded in nuisance for no court would regard the taking of a single photograph as an actionable nuisance. But if the circumstances were such that a plaintiff was subjected to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity, I am far from saying that the court would not regard such a monstrous invasion of his privacy as an actionable nuisance …

88 (1991) 23 NSWLR 443 (NSW SC).

89 Defamation Act 1992, s 8(1).

90 Defamation Act 1992, s 9.

91 *CW Wah Jang and Co Ltd v West* [1933] NZLR 235.

92 Defamation Act 1992, s 6.

93 [1978] QB 479, 489.

2.88 An interim injunction was awarded in *Hubbard v Pitt*[94] against defendants who were protesting outside the plaintiff's business to an extent that they were "watching and besetting" the plaintiff's premises. There, however, the injunction was granted on the basis of serious interference with the plaintiff's business, rather than expressly on privacy grounds.

2.89 In 1976, the Alberta Court of Appeal in *Motherwell v Motherwell* recognised invasions of privacy by way of abuse of the telephone system as a new category of private nuisance.[95] There, the plaintiff was subjected to deliberate and persistent harassment by repeated telephone calls. The decision was relied upon by the English Court of Appeal in *Khorasandjian v Bush*,[96] which arose from similar circumstances.

2.90 In New South Wales, an action in nuisance was used to obtain an interim injunction by plaintiffs whose neighbour trained movement-activated video surveillance equipment and lights on their backyard. While the judge noted that photographing a person was not actionable per se, he considered that there were some limits on the freedom to photograph and, by analogy with *Motherwell* and *Khorasandjian*, was prepared to find the use of video equipment to be sufficiently close to grant the injunction.[97] It seems that there would need to be some form of persistent spying: the tort cannot be used to prevent a neighbour from looking over the fence to see what is happening next door.[98]

2.91 An action for nuisance is based on the protection of property interests and so is limited to those who have an interest in the land in question. The House of Lords overruled *Khorasandjian* on this point in *Hunter v Canary Wharf Ltd*.[99] Thus, it seems that a recipient of harassing telephone calls and other forms of privacy invasion would need to have an actual interest in the land in question and cannot be a mere licensee.[100]

2.92 An action for nuisance also requires proof of actual or imminent harm, however, the courts appear to have had little trouble in finding the stress and emotional harm involved in the harassment and persistent invasion of privacy to be sufficient.

Harassment

2.93 Complaints of interference with privacy may arise from a fear for the safety of the complainant, or from a pattern of harassment that causes anxiety and distress, and these may be covered by the Harassment Act 1997.[101]

---

94 [1976] QB 142 (EWCA).

95 *Motherwell v Motherwell* (1976) 73 DLR (3d) 62 (Alb SC, App Div).

96 [1993] QB 727 (EWCA).

97 *Raciti v Hughes* (1995) 7 BPR 14, 837 (NSW SC) Young J. See also John Gaudin "Comment: *Raciti v Hughes*" [1996] PLPR 8.

98 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 (HCA).

99 [1997] AC 655 (HL).

100 The successful plaintiff in *Khorasandjian* had been the daughter of the woman at whose house the telephone calls had been received, and thus had no proprietary interest in the property herself.

101 In *Hosking v Runting* [2005] 1 NZLR 1, paras 106-108, Gault P and Blanchard J noted that this Act was among the legislative provisions that recognise the privacy value and entitlement to protection.

The Act provides for both civil and criminal penalties for various types of harassment. The key feature of that Act is that the complainant must establish a pattern of behaviour rather than a single intrusion.

2.94 Under the terms of the Act, a person harasses another if he or she engages in a pattern of behaviour, directed against that other person, that includes doing any of the acts specified in the legislation to the other person on at least two separate occasions within a period of 12 months.[102] The specified acts need not be done to the same person on each occasion, as long as the pattern of behaviour is directed against the same person.[103] The legislation specifies the following acts:[104]

- watching, loitering near, or preventing or hindering access to or from, the person in question's place of residence, business, employment, or any other place that the person frequents for any purpose;
- following, stopping, or accosting that person;
- entering or interfering with property in that person's possession;
- making contact with that person, whether by telephone, correspondence, or in any other way;
- 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; and
- acting in any other way that causes the person in question to fear for his or her safety, and that would cause a reasonable person in those circumstances to fear for his or her safety.

2.95 Restraining orders can be granted under Part 3 of the Act. A District Court may make a restraining order if it is satisfied that the respondent has harassed or is harassing the applicant, that an order is necessary to protect the applicant from further harassment, and that the following requirements are met: first, the behaviour in question causes or threatens to cause distress to the applicant; second, that behaviour would cause, or threaten to cause, distress to a reasonable person in the applicant's particular circumstances; and third, in all the circumstances the degree of distress caused or threatened by that behaviour justifies the making of the order.[105] Breach of an order is punishable by a maximum term of imprisonment of six months or a fine not exceeding $5000.

2.96 It may also be that *Khorasandjian*, discussed above, is better viewed as suggesting the existence of a tort of intentional harassment.[106]

Malicious falsehood

2.97 At common law, proceedings will lie for a written or oral falsehood, published maliciously, which is calculated in the ordinary course of things to produce, and does produce, actual damage.[107] An injunction was granted on the basis of

102 Section 3(1).

103 Section 3(2)(b).

104 Section 4(1)(a)–(f).

105 Section 16(1).

106 In *Hunter*, Lords Hoffman, Goff and Lloyd made reference to the case as a harassment matter. See *Hunter v Canary Wharf Ltd* [1997] AC 655, 691, 698 and 707.

107 *White v Mellin* [1895] AC 154, 160, 166, and 167.

malicious falsehood in the English case of *Kaye v Robertson*[108] in a manner which indirectly protected the plaintiff's privacy. The plaintiff was a well-known actor who had a car accident that resulted in severe head and brain injuries. A journalist and photographer, ignoring the warnings regarding visitation restrictions, surreptitiously entered the plaintiff's room. They interviewed him and took photographs, including some showing substantial scars to his head. The defendants claimed that the plaintiff agreed to be interviewed, but medical evidence was later presented that showed that the plaintiff was not fit to be interviewed or to consent to the interview.

2.98 The Court of Appeal felt unable to rely on other causes of action (including trespass to land, below) and held that there was no right of privacy in English law. Instead, the injunction was granted on the basis that the article's claim that the plaintiff had consented to be interviewed was false and resulted in damage, namely, the potential loss of the plaintiff's right to sell the story of the accident and his recovery if the defendants were able to publish their article.

Trespass

2.99 Damages for *trespass to land* have included compensation for an invasion of privacy. In *Ramsay v Cooke*,[109] Holland J held that landowners whose land had been repeatedly trespassed upon were "clearly entitled to damages because of their loss of privacy and their rights as landowners to keep others off". A permanent injunction was also granted restraining the defendants from further trespassing.

2.100 In so far as privacy intrusions are concerned, the action is limited in that it requires an unlawful entry on to land, and can only be brought by the possessor of the land.[110] In *Hosking*, Gault P and Blanchard J suggested that the action is therefore of limited value in protecting against information obtained surreptitiously because modern methods of audio and visual surveillance could be used without committing a trespass.[111]

2.101 However, a line of Australian cases have accepted that the action may be used as a means of obtaining an injunction to prevent publication of information obtained during a trespass, where publication would be "unconscionable". Thus in *Emcorp Pty Ltd v Australian Broadcasting Corporation*, the defendant television corporation was restrained from publishing or disseminating any video, film or sound recording taken during the reporter's presence on the plaintiff's premises.[112]

---

108 [1991] FSR 62 (EWCA Civ).

109 [1984] 2 NZLR 680, 687 (HC). See also *Greig v Greig* [1966] ALR 989 (Vic SC) where nominal damages were awarded for "indignation at the defendant's intrusion into ... privacy" after the defendant entered private property to install surveillance equipment; *Brankin v MacLean* [2003] 2 NZLR 687, 712, John Hansen J (HC).

110 See *Kaye v Robertson* [1991] FSR 62 (EWCA Civ).

111 *Hosking v Runting* [2005] 1 NZLR 1, para 118, Gault P and Blanchard J.

112 *Emcorp Pty Ltd v Australian Broadcasting Corporation* [1988] 2 Qd R 169. See also *Lincoln Hunt Australia Pty Ltd v Willesee* (1986) 4 NSWLR 457; *Whiskisoda Pty Ltd v HSV Channel 7 Pty Ltd* (5 November 1993) Vic SC 9417/93, McDonald J; and *Church of Scientology Inc v Transmedia Productions Pty Ltd* [1987] Aust Torts Rep 68,637.

2.102 It is in theory possible, even after the accident compensation legislation, to sue for *trespass to the person*. This tort is actionable per se, and does not require proof of damage. Even a touching not causing any injury is actionable. An invasion of privacy, such for example as an unauthorised body search, might give rise to such a cause of action.[113]

2.103 In the same way, *trespass to goods* remains a tort New Zealand. Its constituent elements are open to more doubt than the other forms of trespass, and it is not clear whether interference with goods without causing damage to them is enough.[114] If it were, the tort might well be constituted by, for example, rummaging in someone else's handbag, or searching someone else's car. Both of these might be categorised as invasions of privacy.

Intentional infliction of harm

2.104 In *Wilkinson v Downton*,[115] decided in 1896, Wright J ruled that liability could lie where a person intentionally inflicted harm on another that did not amount to a trespass to the person. In that case, the defendant told the plaintiff that her husband had been seriously injured, intending that she should believe it. The plaintiff suffered a violent emotional reaction causing her to become ill.[116]

2.105 In New Zealand in 1985 the rule in *Wilkinson* was relied on to protect privacy interests. In *Tucker*, Jeffries J accepted the argument that the tort of intentional infliction of emotional distress or physical damage could be applied to protect privacy interests. He considered the existence of a tort of invasion of privacy to be a natural progression from the *Wilkinson* tort:[117]

> The gist of the action, unlike defamation, is not injury to character or reputation, but to one's feelings and peace of mind. … The gravamen of the action is unwarranted publication of intimate details of the plaintiff's private life which are outside the realm of legitimate public concern, or curiosity. … In my view the right to privacy in the circumstances before the Court may provide the plaintiff with a valid cause of action in this country. It seems a natural progression of the tort of intentional infliction of emotional distress and in accordance with the renowned ability of the common law to provide a remedy for a wrong.

2.106 In *Tucker* there had been evidence before the court that publication of details about the plaintiff's previous convictions could have a lethal effect on his health at a time when he was awaiting a heart transplant. The Court of Appeal agreed, with some reservations, that the facts of the case raised serious arguable issues. In a subsequent hearing of an application to discharge the interim

113 *Craig v Attorney-General* (1986) 2 LRNZ 551.

114 *Everitt v Martin* [1953] NZLR 298; *Wilson v New Brighton Panelbeaters Ltd* [1989] 1 NZLR 74.

115 [1897] 2 QB 57.

116 The rule was applied in New Zealand in *Stevenson v Basham* [1922] NZLR 225 where a landlord's threat caused a woman to become upset and suffer a miscarriage.

117 *Tucker v News Media Ownership Ltd* (22 October 1986) HC WN CP 477-86, Jeffries J; cited in *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716 McGechan J.

injunctions that had been granted, McGechan J considered that it was not beyond the common law to adapt the *Wilkinson* principles to develop a tort of invasion of personal privacy.[118]

2.107 However, in the United Kingdom the utility of the rule in *Wilkinson v Downton* has been doubted. In *Wainwright v Home Office*,[119] Lord Hoffman noted Hale LJ's finding in *Wong v Parkside Health NHS Trust* that damages for distress falling short of psychiatric injury could not be recovered even where there was an intention to cause it. Further, since damages could be sought for nervous shock (that is actual psychiatric injury) caused by negligence, it was questionable whether there was a need for the intentional *Wilkinson* tort. Nevertheless, Lord Hoffman did not entirely close the door to a tort based on the principles in *Wilkinson*. While he reserved his opinion on the matter, he did not rule out that there could be a claim for compensation for mere distress. However, if such a claim were ever to succeed, the degree of intention required would have to exceed imputed intention, as was the case in *Wilkinson* itself. The defendant, he considered, would have to have acted in a way he or she knew to be unjustifiable and intended to cause harm, or at least to have acted without caring whether he or she caused harm or not. Further, Lord Hoffman noted reservations that behaviour that showed a lack of consideration and appalling manners should be dealt with by way of litigation.

2.108 The result is that the potential for *Wilkinson* is now questionable and at best very narrow. Further, given the recognition in New Zealand common law of a distinct tort of invasion of privacy, arguably it may be of no further use.

Negligence

2.109 As noted above, damages can be sought for nervous shock caused by negligence, and while such claims are likely to be rare, it is possible that such a claim could protect privacy interests. An example is *Furniss v Fitchett*,[120] where a woman's doctor gave a medical certificate relating to her delicate emotional state to her estranged husband. The court found that it was reasonably foreseeable that the contents of the certificate would come to the woman's attention because of the disclosure and that she would be likely to suffer harm, in the form of shock, as a result.

2.110 In *G v Attorney-General*,[121] the Court refused to strike out a claim in negligence against the Department of Social Welfare for wrongly disclosing to an adopted child that the plaintiff was his natural mother. The Court considered that both emotional harm to the mother and subsequent economic loss in taking steps to restore or achieve anonymity could easily have been contemplated.

118 *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716, 733 McGechan J.

119 [2004] 2 AC 406, para 41 (HL) Lord Hoffman, citing with approval *Wong v Parkside Health NHS Trust* [2003] 3 All ER 932 (CA). In *Wainwright*, Lord Hoffman concluded that, in any event, the intention required under the *Wilkinson* tort was not present.

120 [1958] NZLR 396 (SC).

121 [1994] 1 NZLR 714 (HC).

Breach of contract

2.111 Claims may also arise from express or implied terms in contracts that a party will not publish or reveal information about the other. In *Pollard v Photographic Co*[122] a photographer who had photographed a woman for payment was restrained from selling or exhibiting copies of the photograph on the basis that there was an implied contract not to use the negatives in that way.

Passing off

2.112 An action for passing off is made out where there is:[123]

> (1) A misrepresentation (2) made by a trader in the course of trade, (3) to prospective customers of his or ultimate consumers of goods or services supplied by him, (4) which is calculated to injure the business or good will of another trader (in the sense that this is a reasonably foreseeable consequence), and (5) which causes actual damage to a business or good will of the trader…

2.113 While actions for passing off normally relate to goodwill in a business, they can arguably protect privacy interests where they concern the appropriation of the name, image or likeness of a person without his or her consent. An Australian example is *Henderson v Radio Corporation Pty Ltd*,[124] where two well-known professional ballroom dancers succeeded in obtaining an injunction to restrain the defendants from releasing a record of ballroom dancing music which displayed their photograph on the cover without their consent. The New South Wales Supreme Court held that the plaintiffs' potential to exploit the goodwill in their names and reputation could be damaged by the defendant's conduct.

Breach of statutory duty

2.114 Sometimes a civil remedy in damages or injunction will lie for breach of a duty prescribed by statute. In some cases the relevant statute expressly provides for such a remedy. Two examples are relevant in the privacy context. The Copyright Act 1994 provides generally for remedies, including damages, in the case of the various breaches of copyright. Section 105 of the Act provides a privacy-related cause of action. It provides that a person, who, for private or domestic purposes, commissions a photograph or film, even if he or she does not own the copyright, has the right:

- not to have the copies issued to the public;
- not to have the work exhibited or shown in public; and
- not to have the work broadcast.

Section 125 provides that the right is actionable, and both damages and injunctive relief are available.

122 (1888) 40 Ch D 345.

123 *Erven Warnink BV v J Townend and Sons (Hull) Ltd* [1979] AC 731, 742 (HL) Lord Diplock.

124 [1960] SR (NSW) 576. See also New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP 1, Sydney, 2007) 49.

2.115 A second example is to be found in the Residential Tenancies Act 1986, which gives some recognition to privacy by requiring that a landlord must not cause or permit any interference with the reasonable peace, comfort or privacy of the tenant in the use of the premises by the tenant.[125] Contravention of that duty in circumstances that amount to harassment is declared to be unlawful, and exemplary damages may be awarded.[126]

2.116 However, there is a much more difficult issue. There is a tort of breach of statutory duty.[127] A court will sometimes find that a civil remedy lies for breach of a statutory provision even though the statute in question does not expressly provide for such a remedy. By no means all statutory duties are thus enforceable: the rule adopted by the courts is that it is only those which on the true construction of the provision in question must have been intended by Parliament to carry a civil remedy. Deciding whether such an intention exists involves a difficult process of interpretation which requires a consideration of the wording of the statutory provision in question; the reason for its enactment; and its purpose.[128]

2.117 Over the years the courts have laid down some tests or guidelines for resolving the question. Thus, statutory provisions which are for the protection of a particular class of persons rather than the public at large are often held to be enforceable by members of the protected class. Again, if the statute expressly provides for other effective methods of enforcement, a civil remedy is less likely to have been intended. It is sometimes said that if a criminal penalty is provided this reduces the likelihood that a civil remedy was intended. The nature of the duty is important too: the less clearly and precisely defined it is, the less likely it is to carry a remedy. The nature of the damage or loss suffered is also relevant: so far the courts have been more willing to find a civil remedy if the loss is clearly measurable in money than if it is of a more intangible kind.

2.118 However useful these guidelines may be, they are just that – guidelines and not rules. They do not inevitably lead the interpreter to the answer. For example, despite the guideline noted above, it is not uncommon for a court to find that a provision providing for a criminal penalty also carries a civil remedy. The best example of that was in the old industrial statutes imposing duties of safety on employers.

2.119 So the outcome of cases on this tort is not readily predictable. Examples of cases where a remedy has been allowed include cases against a local authority for providing an inaccurate Land Information Memorandum report under the local government legislation,[129] and against the vendor under a hire purchase agreement who repossessed and resold the goods in breach of the hire purchase

125 Residential Tenancies Act 1986, s 38. See also ss 40(2)(b) and 45(1)(e).

126 Residential Tenancies Act 1986, s 109.

127 See John Burrows "Breach of Statutory Duty" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 337.

128 The leading modern authorities are *X (Minors) v Bedfordshire Country Council* [1995] 2 AC 633; *R v Deputy Governor of Parkhurst Prison, ex parte Hague* [1992] 1 AC 58 and, in New Zealand, *Select 2000 Ltd v ENZA Ltd* [2002] 2 NZLR 367 (CA).

129 *Altimarloch Joint Venture Ltd v Moorhouse* (3 July 2008) HC BLE CIV 2005-406-91.

legislation.[130] On the other hand, actions have failed for breaches of the Resource Management Act,[131] and for breaches of duty on the part of those administering the parole legislation.[132]

2.120 As we discuss below, there are a number of criminal statutes which protect privacy. There is a possibility, as yet untested, that some of them might be held to carry a civil remedy for their breach as well. Among them might perhaps be the provisions of the Crimes Act dealing with intimate covert filming, and those prohibiting the interception of private conversations. There is some authority in Australia suggesting that an injunction may lie on the latter type of statute.[133] The uncertainty inherent in this branch of the law is unsatisfactory. One of the questions we shall be considering in this paper is whether damages or injunction should lie for a breach of some criminal statutes which protect privacy, and if so whether this should not be spelled out expressly in the legislation itself. Such certainty might be beneficial.

CRIMINAL OFFENCES

2.121 New Zealand has a number of criminal offences that protect privacy interests in some way. This section details the existing criminal law as it relates to privacy. Later in this paper we consider what the role of the criminal law should be in protecting privacy, and whether the existing criminal offences are adequate. Some of the offences described may not have been intended primarily to protect privacy interests, and some are only peripherally relevant to privacy. However, we have tried to include all provisions that could be seen as providing some protection for privacy, to give a complete picture of the protection offered by the criminal law.

Provisions criminalising invasions of privacy

Offences related to intrusion

2.122 A number of provisions criminalise what could be characterised as intrusions into people's privacy, such as looking into their homes, photographing or filming them without their consent, trespassing on their property, or harassing them.

2.123 Section 30 of the Summary Offences Act 1981 creates an offence of peeping or peering into a dwelling house, or loitering on any land on which a dwelling house is situated, by night and without reasonable excuse. The penalty is a fine not exceeding $500. It is important to note that this provision does not provide any protection where the peeping, peering or loitering occurs during the day. This seems somewhat anomalous, as peeping or peering into a person's house, or loitering on the land on which it is situated, during the day could be just as serious an intrusion into their privacy as if it occurred at night.

2.124 Section 52 of the Private Investigators and Security Guards Act 1974 provides that private investigators may not take or cause to be taken, or use or accept for use, any photograph, film or video recording of another person (except for the

130 *Harris v Lombard New Zealand Ltd* [1974] 2 NZLR 161.

131 *Mawhinney v Waitakere City Council* (14 September 2006) HC AK CIV 1999-404-001850.

132 *Hobson v Attorney-General* [2005] 2 NZLR 220.

133 *Shiel v Transmedia Productions Pty Ltd* [1987] 1 Qd R 199.

purpose of identifying a person on whom a legal process is to be served). They also may not record the voice or speech of another person using a mechanical device. However, they may do these things with the person's prior written consent. The penalty for this offence is a fine of up to $2000.[134]

2.125 Section 141(1)(f) of the Corrections Act 2004 provides that it is an offence to make a visual recording (including a photograph, video or film) or sound recording of a prisoner if making the recording may prejudice the maintenance of the law, the safe custody of the prisoner, the safety of any person or the security of the prison. The penalty is a fine of $2000, imprisonment for up to three months, or both.

2.126 It is an offence under section 4(1) of the Summary Offences Act 1981 to behave in an offensive or disorderly manner in, or within view of, a public place. It was held to be an offence under this section when a man was seen taking photographs of school girls through a gap in curtains in a parked vehicle.[135] While there was a privacy-related element here, the essence of the offence is not so much any invasion of privacy in itself, as the fact that the conduct would arouse anger, disgust or outrage in a reasonable person.

Intimate covert filming

2.127 The Crimes (Intimate Covert Filming) Amendment Act 2006 inserted sections 216G to 216N into the Crimes Act 1961, following recommendations from the Law Commission.[136] These provisions create a regime prohibiting intimate visual recording, defined as:[137]

> A visual recording (for example, a photograph, videotape or digital image) that is made in any medium using any device without the knowledge or consent of the person who is the subject of the recording, and the recording is of –
>
> (a) 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; or
>
> (b) a person's naked or undergarment-clad genitals, pubic area, buttocks or female breasts which is made –
>
> (i) from beneath or under a person's clothing; or
>
> (ii) through a person's outer clothing in circumstances where it is unreasonable to do so.

2.128 There are a number of offences dealing with intimate visual recordings. These are:

134 Private Investigators and Security Guards Act 1974, s 70.

135 *R v Rowe* [2005] 2 NZLR 833. See also *Brooker v Police* [2007] 3 NZLR 91, which affirms that disorderly conduct means disruption of public order.

136 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004).

137 Crimes Act 1961, s 216G.

- making an intimate visual recording intentionally or recklessly;[138]
- possessing an intimate visual recording for the purpose of publishing, exporting or selling it, knowing that it is an intimate visual recording or being reckless as to whether it is;[139]
- possessing an intimate visual recording without reasonable excuse, and knowing that it is an intimate visual recording;[140] and
- publishing, importing, exporting or selling an intimate visual recording, knowing that it is an intimate visual recording or being reckless as to whether it is.[141]

All offences carry a penalty of imprisonment for a term not exceeding three years, except for simple possession of an intimate visual recording (which is punishable by imprisonment for up to a year). There are exceptions for things done in the course of exercising any powers, duties or functions under law. Police, customs officers, officers of the New Zealand Security Intelligence Service, employees of the Department of Corrections, and lawyers giving legal advice in relation to intimate visual recordings are protected from liability.[142]

2.129 In addition to or instead of any other sentence, the Court may order that the intimate visual recording be destroyed within ten working days, and that it is impounded in the meantime. The court may also order that any equipment, goods or other thing used in the commission of the offence be forfeited to the Crown.[143]

Trespass

2.130 It is an offence to trespass on any place and, after being warned to leave by the owner, to neglect or refuse to leave.[144] This is punishable by a fine not exceeding $1000 or imprisonment for a term not exceeding three months.[145] The Trespass Act 1980 also provides for a number of related offences.

2.131 Similarly, a person who is found in or on a building, in an enclosed yard or other area, or in or on any aircraft, hovercraft, ship, ferry or other vessel, train or vehicle commits an offence. The penalty is imprisonment for up to three months or a fine of up to $2000.[146] While these provisions do offer some protection against intrusion where this occurs on a person's property, they are probably directed primarily at protecting property rights rather than privacy.

Harassment and related offences

2.132 The Harassment Act 1997 provides that it is an offence to harass another person where the harasser intends the harassment to cause the person to fear for his or her safety or the safety of a family member, or where the harasser knows that

138 Crimes Act 1961, s 216H.
139 Crimes Act 1961, s 216I(1).
140 Crimes Act 1961, s 216I(2).
141 Crimes Act 1961, s 216J.
142 Crimes Act 1961, s 216N.
143 Crimes Act 1961, s 216L.
144 Trespass Act 1980, s 3.
145 Trespass Act 1980, s 11.
146 Summary Offences Act 1981, s 29.

this is likely to be the result, given the person's circumstances. The penalty is imprisonment for a term of up to two years.[147] Harassment is defined as a pattern of behaviour that includes doing any specified acts on at least two separate occasions within a 12-month period.[148]

2.133 Other offences deal with similar behaviour. Section 112 of the Telecommunications Act 2001 provides that it is an offence to use, or cause or permit to be used, a telephone device for the purpose of disturbing, annoying or irritating any person, whether by calling without speech or by wantonly or maliciously transmitting communications or sounds, with the intention of offending the recipient. It is also an offence to use profane, indecent or obscene language over the telephone with the intention of offending the recipient.

Offences relating to intercepting or interfering with private communications

2.134 A number of criminal offences protect the privacy of communications. Existing offences cover using an interception device to intercept private communications, unauthorised access to computers and opening mail addressed to another person.

Crimes Act 1961, Part 9A

2.135 Part 9A of the Crimes Act 1961, entitled "Crimes against personal privacy", protects private communications through regulating the use of interception devices.

2.136 It is an offence, punishable by up to two years' imprisonment, to intercept any private communication using an interception device, unless the person intercepting the communication is a party to that communication.[149] A private communication is defined as a communication (oral, written or otherwise) made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication. It does not include communications occurring in circumstances where any party ought reasonably to expect that the communication may be intercepted. An interception device is any electronic, mechanical, electromagnetic, optical or electro-optical instrument, apparatus, equipment or other device capable of being used to intercept a private communication.[150]

2.137 The Act creates further related offences. Where a private communication has been intercepted contrary to the Act, it is prohibited to intentionally disclose the communication or its substance or meaning, or to intentionally disclose the existence of the communication, if the discloser knows that the communication has come to his or her knowledge as a direct or indirect result of contravening the Act. The penalty is imprisonment for up to two years.[151] It is also an offence to invite another person to acquire an interception device, offer a device for sale or supply, sell or supply a device or possess a device for the purpose of sale or

147 Harassment Act 1997, s 8.

148 Harassment Act 1997, ss 3 and 4. The specified acts are listed in paragraph 2.94 above.

149 Crimes Act 1961, s 216B.

150 Crimes Act 1961, s 216A.

151 Crimes Act 1961, s 216C.

supply. Again, the penalty is up to two years' imprisonment.[152] As a part of the sentence for offences under section 216B or 216D, the court may order that interception devices be forfeited to the Crown.[153]

2.138 Part 11A of the Crimes Act 1961 provides rules for obtaining interception warrants, so that private communications can be intercepted if necessary for law enforcement purposes. Interception warrants are available for investigating offences involving organised criminal enterprises, serious violent offences and terrorist offences.[154] A judge must be satisfied that it is in the best interests of the administration of justice to grant a warrant. There also must be reasonable grounds for believing that the relevant offence has been or will be committed; that relevant evidence will be obtained through the use of an interception device; and that other investigative procedures and techniques have failed, would be impracticable given the urgency of the situation, or are unlikely to enable the police to successfully investigate.[155] Information obtained must be destroyed as soon as it is no longer required as evidence in proceedings, or if it is irrelevant.[156] Evidence intercepted without an interception warrant is inadmissible in court.[157] Law enforcement officers also may not disclose communications intercepted under a warrant otherwise than in the performance of their duty.[158]

Crimes Act 1961, Part 10

2.139 Part 10 of the Crimes Act 1961 sets out offences relating to computers. Section 252 provides that persons who intentionally access a computer system, directly or indirectly, without authorisation, knowing that they are not authorised to access the computer system or being reckless as to whether they are authorised, commit an offence. The penalty is imprisonment for up to two years. There are qualified exemptions to this provision for the New Zealand Security Intelligence Service and the Government Communications Security Bureau.[159]

Postal Services Act 1998

2.140 Section 23 of the Postal Services Act 1998 provides that it is an offence to, wilfully and without reasonable excuse, open or cause to be opened any postal article not addressed to the person who opens it. The penalty is imprisonment for up to six months or a fine of up to $5000.

Corrections Act 2004

2.141 The Corrections Act 2004 sets out rules governing monitoring of prisoners. While prisoners are subject to greater monitoring than other citizens, these provisions preserve some privacy. Prisoners' telephone calls can generally be monitored, unless they are classified as exempt calls (including calls to

152 Crimes Act 1961, s 216D.

153 Crimes Act 1961, s 216E.

154 Crimes Act 1961, ss 312B, 312CA and 312CC.

155 Crimes Act 1961, ss 312C, 312CB and 312CD.

156 Crimes Act 1961, ss 312I and 312J.

157 Crimes Act 1961, s 312M.

158 Crimes Act 1961, s 312K.

159 Crimes Act 1961, ss 253 and 254.

lawyers, members of Parliament and official agencies).[160] However, there are fairly strict rules around this monitoring.[161] It is an offence to knowingly disclose information obtained through monitoring of prisoners' calls, the penalty being a fine of up to $2000.[162]

Offences involving disclosure and use of private information

2.142 New Zealand law contains many provisions that protect private information by criminalising certain disclosures of information. Sometimes disclosure of information is permitted for a limited purpose but it is an offence to use the information for other purposes once it has been disclosed. This type of offence can be used to allow a certain disclosure that is in the public interest, but to prevent any further use that is not. The offences under the Electoral Act outlined below are examples.[163]

2.143 The Resource Management Act 1991 provides that a local authority may make an order prohibiting or restricting the publication of certain information, where the order is necessary to avoid serious offence to tikanga Māori or to avoid the disclosure of the location of waahi tapu, or to avoid the disclosure of a trade secret.[164] It is an offence to contravene or permit contravention of such an order.[165] The penalty is a fine of no more than $10,000. If the offence is continuing, the offender may be fined up to $1000 for every day the offence continues.[166]

2.144 A person who receives a radio communication and makes use of it, reproduces it or discloses its existence, knowing that he or she is not the intended recipient, commits an offence.[167] The penalty is $30,000 for an individual or $200,000 for a body corporate.[168]

2.145 Similarly, section 20(2) of the Postal Services Act 1998 provides that a person who examines the contents of a postal article without reasonable excuse and divulges without reasonable excuse any information obtained commits an offence. This is punishable by up to six months' imprisonment or a fine of up to $5000.

2.146 The National Cervical Screening Programme, established under Part 4A of the Health Act 1956, involves the collection of personal information, and there are provisions in the Act governing the use and disclosure of this information.

160 Corrections Act 2004, ss 113 and 114.

161 See, eg, Corrections Act 2004, ss 115, 116 and 120.

162 Corrections Act 2004, ss 118 and 146.

163 See also Transport Accident Investigation Commission Act 1990, Part 3.

164 Resource Management Act 1991, s 42.

165 Resource Management Act 1991, s 338(2).

166 Resource Management Act 1991, s 339(2).

167 Radiocommunications Act 1989, s 133A.

168 Radiocommunications Act 1989, s 128.

Certain information held under the Programme must not be disclosed, other than in certain specified situations.[169] Non-compliance with these requirements without reasonable excuse is an offence, incurring a fine of up to $10,000.[170]

2.147 Under the Electoral Act 1993 people may request the Chief Registrar to supply information about electors, including their name, address, occupation, age group and whether they are of Māori descent, for the purposes of scientific research or research into human health.[171] Local government electoral officials may also request this type information for the purposes of elections, by-elections and polls.[172] This information may also be given to political party candidates, members of Parliament, Electoral Commission officials and other people involved in publicity campaigns relating to electoral matters or elections.[173] It is an offence to knowingly and wilfully supply, receive or use this information for an unauthorised purpose. The penalty is $50,000, in the case of information used for commercial purposes, or $10,000 in the case of other purposes.[174] It is also an offence to supply, receive or misuse information about Māori iwi affiliations for purposes other than those authorised by the Act.[175]

2.148 The Electoral Act also protects the secrecy of voting. Electoral officials must only use or disclose information they obtain in accordance with their official duties. Furthermore, people in attendance at the counting of votes must maintain the secrecy of the voting, and must not disclose the contents of particular ballot papers.[176] It is an offence to contravene these provisions, with a penalty of up to two years' imprisonment, a fine of up to $40,000, or both.[177]

2.149 Under section 9 of the Remuneration Authority Act 1977, members of the Authority and others engaged in its work must maintain the secrecy of all matters that come to their knowledge in carrying out their functions and shall not communicate this information except in the discharge of their functions and duties under the Act. This is intended to protect privacy. The penalty is imprisonment for a term of no more than three months, or a fine of up to $1000, or both.

2.150 The New Zealand Public Health and Disability Act 2000 establishes Mortality Review Committees to report on deaths. It is an offence to disclose personal information given to a Mortality Review Committee, carrying a penalty of up to $10,000.[178]

2.151 Under the Judicial Conduct Commissioner and Judicial Conduct Panel Act 2004, the Judicial Conduct Panel may make an order prohibiting publication of records of proceedings before it, documents produced at any hearing or the name and

169 Health Act 1956, ss 112J, 112Y and 112Z.

170 Health Act 1956, s 112ZP.

171 Electoral Act 1993, s 112.

172 Electoral Act 1993, s 113.

173 Electoral Act 1993, s 114.

174 Electoral Act 1993, s 116.

175 Electoral Act 1993, s 117A.

176 Electoral Act 1993, s 203.

177 Electoral Act 1993, s 224.

178 New Zealand Public Health and Disability Act 2000, s 18(7).

details of the affairs of any person. The privacy of the complainant is a relevant factor for the Panel to consider in making an order. It is an offence to contravene an order. The penalty for an individual is a fine of up to $3000, or up to $10,000 for a body corporate.[179]

2.152 Section 105A of the Crimes Act 1961 provides that it is an offence for officials to corruptly use or disclose information that they have acquired in their official capacity to obtain an advantage or pecuniary gain. It is also an offence for someone who has received personal information, knowing that the information has been disclosed in contravention of section 105A, to use or disclose the information to obtain an advantage or pecuniary gain.[180] Both offences are punishable by up to seven years' imprisonment.

2.153 The Criminal Investigations (Bodily Samples) Act 1995 contains a number of provisions relating to the privacy of suspects giving DNA samples for the purpose of criminal investigations. Where an application is made for an order authorising the taking of a bodily sample, no person may publish the name of the respondent or any name or details likely to lead to the identification of the respondent unless a High Court Judge permits it, or the respondent is charged.[181] Where the application relates to a person under the age of 17, no person may publish the name of the respondent or his or her parents or caregivers.[182] The penalty is a fine of up to $1000.[183] The Act also provides that it is an offence to access information stored on a DNA profile databank or to disclose this information, except for certain specified purposes.[184] The penalty is imprisonment for a term of up to three years.[185]

2.154 Section 13(8) of the Parole Act 2002 provides that it is an offence to publish information provided by the Parole Board to the offender in a form that identifies or enables the identification of the victim. The penalty for an individual is up to three months' imprisonment or a fine of up to $2000, and for a body corporate it is a fine of up to $10,000.

2.155 A number of Acts contain offence provisions for the publication of material obtained under interception warrants. Under section 23 of the Misuse of Drugs Amendment Act 1978, a person who knowingly discloses a private communication obtained under an interception warrant is liable to a fine of up to $500. Section 312K of the Crimes Act 1961 has the same effect. Section 12A of the New Zealand Security Intelligence Service Act 1969 provides that it is an offence for officers or employees to disclose or use information obtained through their connection with the Service, other than in the course of their official duties. It is also an offence to disclose information obtained through an interception warrant, except as authorised by the warrant or the Minister or Director. The penalty is up to two years' imprisonment or a fine of up to $2000.

179 Judicial Conduct Commissioner and Judicial Conduct Panel Act 2004, s 30.

180 Crimes Act 1961, s 105B.

181 Criminal Investigations (Bodily Samples) Act 1995, s 14.

182 Criminal Investigations (Bodily Samples) Act 1995, s 19.

183 Criminal Investigations (Bodily Samples) Act 1995, s 77.

184 Criminal Investigations (Bodily Samples) Act 1995, s 27.

185 Criminal Investigations (Bodily Samples) Act 1995, s 77.

2.156 Under the Criminal Records (Clean Slate) Act 2004, it is an offence for persons to disclose information about an individual's criminal record that is required to be concealed, knowing that they do not have lawful authority to do so, or being reckless as to whether they have authority.[186]

2.157 A number of statutes contain prohibitions on publication, or powers to prohibit the publication, of names, evidence or submissions in court proceedings. For example, under the Criminal Justice Act 1985 a court may make orders clearing the court or prohibiting the publication of records of the proceedings, the name of the accused, the names of witnesses or details likely to lead to the identification of witnesses. The Act also prohibits the publication of names of victims or the accused in cases involving certain sexual offences. It is an offence, punishable by a fine of up to $1000, to breach an order.[187] No person may publish the name of a child witness in criminal proceedings, or details likely to lead to the identification of the child. Individuals may be punished by a fine of up to $1000 or imprisonment for up to three months, and bodies corporate by a fine of up to $5000, for contravening this prohibition.[188]

2.158 Suppression, for the most part, is not directed at protecting privacy. The public interest in open justice has traditionally been taken to be the overriding concern. Until recently, privacy was not considered a directly relevant factor in the balancing exercise, although it could be taken into account.[189] However, recent cases suggest that privacy considerations are becoming increasingly relevant in decisions about suppression.[190]

2.159 A significant number of statutes contain offences for disclosing information obtained in the course of business or employment. These are probably directed at protecting trade secrets and confidentiality more than privacy, but confidentiality and privacy overlap and there is not always a clear boundary between the two. Some examples follow of offences relating to information obtained by officials of particular public agencies.

2.160 Part 4 of the Tax Administration Act 1994 contains provisions directed at maintaining secrecy of tax information. The Act sets out specified situations in which information may be disclosed. It is an offence to fail to maintain secrecy outside these situations. The penalty is imprisonment for up to six months, a fine of up to $15,000, or both.[191]

186 Criminal Records (Clean Slate) Act 2004, s 17.

187 Criminal Justice Act 1985, ss 138, 139 and 140.

188 Criminal Justice Act 1985, s 139A.

189 See, eg, *Re Victim X* [2003] 3 NZLR 220 (CA), discussed in Robert Stewart "Suppression and Contempt" in *Media Law – Rapid Change, Recent Developments* (New Zealand Law Society, 2008) 14-15.

190 See, eg, *J v Serious Fraud Office* (10 October 2001) HC AK A126/01, Baragwanath J. See also New Zealand Law Commission *Suppressing Names and Evidence* (NZLC IP 13, Wellington, 2008).

191 Tax Administration Act 1994, ss 143C and 143D.

2.161 Under section 21 of the Statistics Act 1975, employees must make a declaration of secrecy in relation to information obtained during the course of their duties. It is an offence to fail to maintain secrecy, or to obtain information without authorisation,[192] with a penalty of up to $500 for an individual or $2000 for a body corporate.[193]

2.162 Similarly, ombudsmen and their officials must maintain secrecy in relation to matters that come to their knowledge in the exercise of their functions, and must take an oath to this effect.[194] It is an offence not to comply, carrying a penalty of a fine of up to $200.[195]

Search and surveillance powers

2.163 In contrast to the above offence provisions that protect privacy, the law also contains provisions empowering law enforcement officers to disturb individuals' privacy where necessary for the prevention, detection and investigation of crime. Generally warrants, for example to search property or intercept communications, are required in order to exercise these powers. To ensure that individual privacy is given proper weight, good cause is required before warrants are issued.[196]

2.164 The Search and Surveillance Powers Bill 2008, currently before the New Zealand Parliament, contains provisions prescribing in detail when such warrants will be required. While it is beyond the scope of this paper to consider these provisions in detail, the criteria used to define the warrant regime have informed our own deliberations.

192 Statistics Act 1975, s 40.

193 Statistics Act 1975, s 47.

194 Ombudsmen Act 1975, s 21.

195 Ombudsmen Act 1975, s 30.

196 See New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007) for detailed consideration of the law relating to these search and surveillance powers.

Chapter 3

The regulatory framework

3.1 In addition to the civil and criminal remedies outlined in chapter 2, various statutes provide protection for privacy interests. There are also self-regulatory schemes that provide for privacy protection. This chapter discusses the Privacy Act 1993, media regulatory bodies, the Health and Disability Commissioner Act 1994, and several industry self-regulatory schemes, which all provide means by which people whose privacy may have been breached can complain and potentially receive a remedy.

PRIVACY ACT 1993

3.2 The Privacy Act 1993 mainly protects privacy of personal information, although aspects of the Act concern privacy in a broader sense. For example, the Privacy Commissioner has functions and powers that relate to privacy generally, not only privacy of personal information.[197] The Act sets out 12 information privacy principles governing the way in which agencies[198] may collect, store, use and disseminate personal information,[199] and also provides for the development of Codes of Practice which modify the application of the principles in certain situations.[200] The Act establishes a complaints process to deal with breaches of principles or Codes of Practice. The complaints process begins with conciliation and investigation by the Privacy Commissioner, and may progress to the Human Rights Review Tribunal if settlement does not occur.

Coverage

Aspects of privacy covered

3.3 The information privacy principles are concerned with the collection, use and disclosure of personal information. For this reason, the Act does not always protect against surveillance and intrusion, as these do not always involve personal information. However, some of the information privacy principles,

197 See Privacy Act 1993, ss 13(1)(g)-13(1)(k) and 13(1)(m)-13(1)(r).

198 "Agency" is defined in the Act as any person or body of persons, whether corporate or unincorporated, and whether in the public sector or private sector, including a government Department.

199 Privacy Act 1993, Part 2.

200 Privacy Act 1993, Part 6.

particularly principles 2, 3 and 4, have quite wide application, so offer some protection against surveillance and intrusion, in so far as these involve collection of personal information.

3.4 Principle 3 provides that where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information;
- the name and address of the agency that is collecting the information and the agency that will hold the information;
- the particular law by or under which the collection of the information is authorised or required (if any), and whether the supply of the information is voluntary or mandatory;
- the consequences (if any) for that individual if all or any part of the requested information is not provided; and
- the individual's rights of access to, and correction of, his or her personal information.

There are a number of exceptions provided. The steps set out above must be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.[201]

3.5 Collection is defined as not including receipt of unsolicited information.[202]

3.6 On its face, principle 3 appears wide enough to cover surveillance, as surveillance activities such as photographing or recording images of people can be seen as collection of personal information.

3.7 The Office of the Privacy Commissioner and the Human Rights Review Tribunal have generally treated recorded surveillance and monitoring activities as collection of personal information directly from individuals. For example, hidden video cameras have been found to be collecting personal information directly, therefore attracting the notification requirements.[203]

3.8 However, some doubt has been cast on whether principle 3 applies to surveillance activity, based on the meaning of "collection" and "directly." Paul Roth has argued that covert surveillance via the use of intermediary techniques or devices such as video cameras does not result in a collection of information. This is because the information is not solicited: there is no request for information and individuals are not aware that their activities are being recorded. Roth further argues that information collected by means of intermediary techniques or devices over which the individual has no control is not information collected directly from the individual. He argues that the words "directly from" suggest that the information is collected in an open rather than surreptitious

201 Privacy Act 1993, s 6.

202 Privacy Act 1993, s 2.

203 Paul Roth *Privacy Law and Practice* (looseleaf, LexisNexis, Wellington, last updated 2007) PVA6.6(c).

way: that the individual is aware of the collection, there is a request for the information, and the individual supplies it. This is not the case where information is collected covertly using surveillance devices. Rather, surveillance devices collect information *about* the individual.[204]

3.9 Roth also suggests that this interpretation is consistent with the OECD guidelines, and furthermore that the legislative history and background to the Act suggest that principle 3 was not intended to cover surveillance.[205]

3.10 The case of *Harder v Proceedings Commissioner*[206] may provide some support for Roth's view. In that case, a solicitor recorded a telephone conversation during which the complainant volunteered personal information, without informing her that she was being recorded. The Court of Appeal held that, because the solicitor had not requested that the complainant provide the information, the information was unsolicited and therefore there was no collection of personal information. Thus, arguably surveillance activities such as video recording similarly do not involve collection of personal information: people who are recorded are not asked to provide information, and cameras and other devices could be seen as simply recording unsolicited information about their activities. However, the case is not necessarily analogous to many surveillance activities. The Court's reasoning seems to have been that Harder made no effort to collect the information from the complainant and merely recorded information that she volunteered. In contrast, it could be argued that many surveillance activities, such as the use of hidden cameras or interception devices, do generally involve a deliberate effort to monitor people and record their activities. As such, the argument that the information collected is unsolicited seems less tenable. On this interpretation, many surveillance activities would involve collection of personal information and the requirements of principle 3 apply accordingly.

3.11 Therefore, while principle 3 is wide enough to cover surveillance activities on its face, there is uncertainty in some quarters as to whether it does. This could lead to principle 3 being interpreted so as not to cover surveillance and intrusion. Its application would benefit from clarification.

3.12 Whichever interpretation is correct, use of surveillance devices could contravene principle 2, which provides that where an agency collects personal information, it must collect the information directly from the individual concerned. There are exceptions (including where compliance would prejudice the purposes of the collection or is not reasonably practicable), so one of these may apply. Again, there could be an argument about the meaning of "collection".

3.13 Principle 4 can also cover surveillance. It provides that personal information shall not be collected by an agency by unlawful means, or by means that, in the circumstances of the case, are unfair or intrude to an unreasonable extent upon

204 Paul Roth *Privacy Law and Practice* (looseleaf, LexisNexis, Wellington, last updated 2007) PVA6.6(c).

205 Paul Roth *Privacy Law and Practice* (looseleaf, LexisNexis, Wellington, last updated 2007) PVA6.6(c).

206 [2000] 3 NZLR 80 (CA).

the personal affairs of the individual concerned.[207] Surveillance that is unlawful, unfair or unreasonably intrusive is covered by principle 4, provided that the surveillance can be said to result in collection of personal information.

3.14 Instances of surreptitious tape or video recording have been found to be unfair under principle 4. In one example, an insurance company engaged a private investigator to investigate a claimant. The private investigator noticed that the claimant's house was for sale and, posing as a potential purchaser, videotaped the claimant in the house under the guise of gathering footage of the house to show to his wife. The insurance company used the footage in an attempt to refute the claimant's claim for permanent disability. The Privacy Commissioner found that this breached principle 4.[208]

Application to the news media

3.15 In many situations, it will not be possible to bring a complaint against the news media under the Privacy Act. This is because the Act exempts from the definition of "agency" any news medium, in relation to its news activities.[209] "News activity" is defined as:

> (a) the gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public:
>
> (b) the dissemination, to the public or any section of the public, of any article or programme of or concerning –
>
> (i) news
>
> (ii) observations on news
>
> (iii) current affairs.

"News medium" is defined as any agency whose business, or part of whose business, consists of a news activity. However, Radio New Zealand and Television New Zealand are not news media in relation to principles 6 and 7, which relate to access to, and correction of, personal information.[210]

3.16 "News activities" has to date been interpreted quite broadly. For example, the Privacy Commissioner formed the opinion that consumer affairs television show *Target*, which had covertly filmed a television technician at work, was news or current affairs and therefore not within the Act.[211] A leading case

207 Privacy Act 1993, s 6.

208 *Man Complains of Unfair Video Recording During Insurance Investigation* [1997] NZPrivCmr 14 – Case Note 14824; Paul Roth *Privacy Law and Practice* (looseleaf, LexisNexis, Wellington, last updated 2007) PVA6.7(d).

209 Privacy Act 1993, s 2(1), definition of "agency", (b)(xiii).

210 Privacy Act 1993, s 2. The reason why principles 6 and 7 apply to Television and Radio New Zealand is that, before the enactment of the Privacy Act, people had the right to seek access to and correction of personal information held by the public broadcasters under the Official Information Act. When the Privacy Act removed the application of the Official Information Act to personal information requests by individuals, this right needed to be placed in the Privacy Act to ensure that the Privacy Act did not remove existing rights.

211 *TV Technician Complains About Being Covertly Filmed for a TV Programme* [2003] NZPrivCmr 24 – Case Note 38197.

is *Talley Family v National Business Review*,[212] in which the then Complaints Review Tribunal (now Human Rights Review Tribunal) considered whether the publication of the "Rich List" was a news activity. It considered two approaches to the interpretation of news activity. First, a broad interpretation, under which the content of the publication is not analysed. The only question under this approach is whether the publication was part of an activity by the defendant broadly described as a news activity, as distinguishable from the news medium's other functions such as advertising and employing staff. The second possible approach involved analysing the content of the publication, applying a public interest test to determine whether it is "news." The Tribunal found that on either approach the publication was a news activity. It did not state clearly which was the correct approach.[213]

3.17 Therefore, it is likely to be difficult to successfully complain to the Privacy Commissioner about a breach of privacy by the news media, except in relation to breaches of principles 6 and 7 by Radio New Zealand or Television New Zealand. We note however that, although the news media are not bound by the Act in relation to their news activities, the Privacy Commissioner may inquire into and comment on media practices affecting the privacy of individuals, even where these relate to the media's news activities.[214] In 2007 the Commissioner reported on her inquiry into the publication of photographs of elderly people and their carers in the journal of the New Zealand Nurses Organisation. The Commissioner noted that, while the journal fell within the definition of news medium and was therefore not subject to the Act's complaints provisions, she was empowered by section 13(1)(m) of the Act to inquire generally into any matter if it appears that individual privacy may be being infringed.[215]

Complaints to Privacy Commissioner

3.18 The information privacy principles are not enforceable in the courts.[216] Rather, breaches of the principles are dealt with through the complaints process outlined in this section. The exception is that the entitlement to access personal information in principle 6, where that information is held by a public sector agency, is a legal right and is enforceable in the courts.[217]

3.19 Any person may make a complaint to the Privacy Commissioner ("the Commissioner") alleging that any action is or appears to be an interference with the privacy of an individual. For the purposes of a complaint, an action is an

212 (1997) 4 HRNZ 72.

213 See also discussion in John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, Melbourne, 2005) 275-277; Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, last updated 2007) PVA2.2(e).

214 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, last updated 2007) PVA2.2(e).

215 Marie Shroff, Privacy Commissioner "Commissioner Initiated Inquiry under Section 13 of the Privacy Act 1993: Publication of Photographs of Elderly People and their Carers" (March 2007) 4.

216 Privacy Act 1993, s 11(2).

217 Privacy Act 1993, s 11(1).

interference with the privacy of an individual if it breaches an information privacy principle, a Code of Practice or Part 10 of the Act (relating to information matching). Furthermore, an action is not a breach of privacy unless it:

- has caused, or may cause, loss, detriment, damage or injury;
- has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations or interests of the complainant; or
- has resulted in, or may result in, significant humiliation, loss of dignity or injury to the feelings of the complainant.[218]

The Act also provides that, in the performance of his or her functions, the Commissioner must have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.[219] This may also affect the interpretation of what amounts to a breach of privacy.

3.20 Complaints most commonly relate to denial of access to personal information requested under principle 6, and disclosure of personal information in breach of principle 11. Complaints about breaches of the other principles are much less common.[220] The Commissioner's functions in relation to complaints are to investigate, act as a conciliator and take such further action as is contemplated by Part 8 of the Act (that is, investigation and settlement of complaints, and action in the Human Rights Review Tribunal).[221]

3.21 The Privacy Commissioner also has complaints resolution functions under other Acts. These include complaints about:

- a health agency's failure to transfer health records;[222]
- refusal to suppress residential details under the Domestic Violence Act 1995;[223]
- breaches of the code of conduct made under the Social Security Act 1964, applying to use of powers to demand certain information;[224]
- certain access requests by non-New Zealanders subject to intercountry adoption orders;[225] and
- decisions under the Human Assisted Reproductive Technology Act 2004 regarding access to or correction of information, and complaints that information has been obtained, kept or disclosed contrary to the provisions of that Act.[226]

Complaints under these Acts are resolved using the Privacy Act complaints process.

---

218 Privacy Act 1993, s 66.

219 Privacy Act 1993, s 14(a).

220 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, last updated 2007) PVA 67.3.

221 Privacy Act 1993, s 69.

222 Health Act 1956, s 22F.

223 Domestic Violence Act 1995, ss 118-120 and Domestic Violence (Public Registers) Regulations 1998, r 11.

224 Social Security Act 1964, s 11B.

225 Adoption (Intercountry) Act 1997, s 13.

226 Human Assisted Reproductive Technology Act 2004, s 66.

3.22 Upon receiving a complaint, the Office of the Privacy Commissioner will assess it against the information privacy principles in order to form a view on whether there has been a breach. They would then consider a range of options to deal with the complaint, ranging from equipping the parties to resolve the issue themselves, to mediation or a full investigation of the complaint. The Office will generally attempt to resolve the dispute at all stages of the process, and in fact most cases are either settled or not pursued further by the complainants after the investigation is completed.[227]

3.23 Where an investigation takes place and the Commissioner is of the opinion that a complaint has substance, she must use her best endeavours to secure a settlement between the parties. If this is unsuccessful, the Commissioner may refer the matter to the Director of Human Rights Proceedings for the purpose of deciding whether proceedings should be instituted.[228]

Human Rights Review Tribunal process

3.24 The Director of Human Rights Proceedings considers the information given by the complainant and the Commissioner, in order to decide whether the case should progress to the Human Rights Review Tribunal ("the Tribunal"). The main consideration in deciding whether to take a case is whether there is evidential sufficiency. If the Director decides to take the case, he acts as the plaintiff, rather than appearing for the complainant.[229]

3.25 Another route to the Tribunal is that an individual may himself or herself bring proceedings if the Commissioner or the Director is of the opinion that the complaint does not have substance or ought not to be proceeded with, or where the Director agrees to the individual bringing proceedings or declines to take proceedings.[230] Agencies may not take proceedings: their only option is to refuse to accept the Commissioner's view and see whether the matter is taken further.[231]

3.26 A complaint must have been investigated by the Commissioner before it can be heard by the Tribunal, regardless of whether the Director or the individual complainant brings the proceedings.

3.27 The Tribunal has had around 18 new proceedings under the Privacy Act per year over the past five years. It issued 14 privacy decisions during the 2006/2007 year.[232]

3.28 The Tribunal considers the matter afresh. The Privacy Commissioner's view of a complaint that has been investigated is not normally relevant. If the Tribunal is satisfied on the balance of probabilities that any action of the defendant is an interference with the privacy of an individual, it may grant:

- a declaration that the action is an interference with the privacy of an individual;

227 Katrine Evans "Show Me the Money: Remedies under the Privacy Act" (2005) 36 VUWLR 475, 480.

228 Privacy Act 1993, s 77.

229 Privacy Act 1993, s 82.

230 Privacy Act 1993, s 83.

231 Katrine Evans "Show Me the Money: Remedies under the Privacy Act" (2005) 36 VUWLR 475, 482.

232 Privacy Commissioner *Annual Report 2007* (Wellington, 2007) 29.

- orders restraining the defendant from continuing or repeating the interference, or requiring the defendant to perform any act specified to redress the interference;
- damages for pecuniary loss, loss of any benefit, or humiliation, loss of dignity, or injury to feelings; or
- such other relief as the Tribunal thinks fit.

The Act provides that it shall not be a defence that the interference was unintentional or without negligence on the part of the defendant, but the Tribunal shall take the conduct of the defendant into account in deciding what, if any, remedy to grant.[233]

3.29 The most commonly awarded remedies appear to be declarations and damages. The Tribunal may award damages of up to $200,000.[234] The highest award of damages so far has been $40,000.[235] Most awards have been below $5000, although it has been suggested that large awards may be becoming more common.[236] The Tribunal has developed some guidance about factors that it will consider in determining the level of damages. The approach may vary somewhat according to which principle is in issue. In *Hamilton v The Deanery 2000 Ltd*,[237] which related to principle 11 (disclosure), it set out the following relevant factors:

- the nature of the agency which disclosed the information;
- whether there were internal standards prescribing an appropriate information handling practice;
- the number of disclosures and width of disclosure;
- the nature of the information;
- motivations of the discloser;
- knowledge of the consequences of the disclosure;
- whether there was an admission of wrongdoing or an attempt to mitigate the injury; and
- knowledge of the legislation.

3.30 If a complainant is not satisfied with the Tribunal's decision, there is a general right of appeal to the High Court.[238] There may be a further appeal with leave, on a question of law, from a decision of the High Court.[239]

HEALTH AND DISABILITY COMMISSIONER ACT 1994

3.31 Complaints can be made to the Health and Disability Commissioner about breaches of the Code of Health and Disability Services Consumers' Rights ("the Code").[240] The Code applies to any person or organisation providing

233 Privacy Act 1993, s 85.

234 Human Rights Act 1993, s 92Q.

235 *Hamilton v The Deanery 2000 Ltd* (29 August 2003) HRRT 36/02, Decision No 28/03.

236 Katrine Evans "Show Me the Money: Remedies under the Privacy Act" (2005) 36 VUWLR 475; Katrine Evans "The Rise and Rise of Damages Awards for Breaches of Privacy? *Hamilton v The Deanery 2000 Ltd*" [2003] PLPR 56.

237 (29 August 2003) HRRT 36/02, Decision No 28/03.

238 Human Rights Act 1993, s 123.

239 Human Rights Act 1993, s 124.

240 For a general description of the complaints process see Health and Disability Commissioner *Complaints Resolution* www.hdc.org.nz/complaints (accessed 19 November 2008).

a health service to the public or a section of the public, or any person or organisation providing a disability service. Right 1(2) provides that every consumer has the right to have his or her privacy respected. This provides another avenue for complaints about breaches of privacy that occur in a health context. In practice, the Health and Disability Commissioner deals with complaints involving physical or spatial privacy, while the Privacy Commissioner deals with complaints relating to privacy of health information.

3.32 Anyone may make a complaint orally or in writing alleging a breach of the Code.[241] Upon receiving a complaint, the Commissioner makes a preliminary assessment of the complaint and decides to refer the complaint to another agency or person, refer the complaint to an advocate, call a conference of the parties, investigate the complaint or take no action.[242] The complaint may also be referred to the Chief Human Rights Commissioner, Privacy Commissioner, Ombudsman, a professional registration authority, the Accident Compensation Corporation, the Director-General of Health or the health or disability service provider.[243]

3.33 About ten per cent of complaints are formally investigated. Before beginning the investigation, the Commissioner informs the parties of his intention to investigate and advises the provider of the details of the complaint.[244] The provider may submit a written response to the complaint. During the investigation, the Commissioner considers oral and documentary evidence. The Commissioner then forms a provisional opinion on whether there has been a breach of the code and notifies the parties of his findings. Parties then have the opportunity to make written submissions on the provisional opinion. Following consideration of these, the Commissioner forms a final opinion.

3.34 Where the Commissioner finds a breach of the Code, actions he may take include making reports and recommendations to the provider, an appropriate authority such as a professional registration body, the Minister of Health or any other person.[245] Where the Commissioner has concerns about the competence of a health practitioner, he may recommend that the relevant registration authority consider whether a review of the practitioner's competence is warranted.

3.35 The Commissioner may also refer the matter to the Director of Proceedings.[246] As in the privacy jurisdiction, the Director of Proceedings may decide to take action in the Human Rights Review Tribunal. The remedies available, as in Privacy Act complaints, include declarations, restraining orders, damages, an order to perform specified acts, or such other relief as the Tribunal thinks fit.[247] The Director can also take disciplinary proceedings against a practitioner in the Health Practitioners Disciplinary Tribunal.[248]

241 Health and Disability Commissioner Act 1994, s 31.

242 Health and Disability Commissioner Act 1994, s 33.

243 Health and Disability Commissioner Act 1994, ss 34 and 36.

244 Health and Disability Commissioner Act 1994, s 41.

245 Health and Disability Commissioner Act 1994, s 45.

246 Health and Disability Commissioner Act 1994, s 45.

247 Health and Disability Commissioner Act 1994, s 54.

248 Health and Disability Commissioner Act 1994, s 49.

MEDIA REGULATION

Broadcasting Standards Authority

3.36 The Broadcasting Act 1989 sets out a complaints process in relation to broadcasters. Every broadcaster is responsible for maintaining, in its programmes and their presentation, standards which are consistent with the privacy of the individual, among other things.[249] The Act then sets out rules concerning complaints, where individuals feel that these standards have not been met.

3.37 First, there is a process for consideration of complaints by broadcasters. Broadcasters must receive and consider formal complaints where it is alleged that they have failed to meet broadcasting standards, and must establish procedures for investigating complaints. Complaints must be submitted within 20 working days of the date on which the programme to which the complaint relates was broadcast.[250] If the broadcaster finds a complaint to be justified, it must take appropriate action and notify the complainant in writing. If not, it must notify the complainant in writing of the decision.[251]

3.38 The Act also establishes an independent Broadcasting Standards Authority (BSA). Complainants may refer their complaints to the BSA if they are dissatisfied with the broadcaster's decision or the action taken, or where the broadcaster has not taken action within 20 working days of receiving the complaint. Complainants are also entitled to complain directly to the Broadcasting Standards Authority, without first complaining to the broadcaster, where the complaint relates to privacy.[252]

3.39 The BSA then considers and determines the complaint. In relation to privacy, it has developed a set of privacy principles that elaborate on what will be considered consistent with the privacy of the individual. These principles, which have been affirmed by the High Court,[253] are based on the jurisprudence around the privacy torts in the United States, and take quite an expansive approach to privacy. The principles are as follows:[254]

(1) It is inconsistent with an individual's privacy to allow the public disclosure of private facts, where the disclosure is highly offensive to an objective reasonable person.

(2) It is inconsistent with an individual's privacy to allow the public disclosure of some kinds of public facts. The "public" facts contemplated concern events (such as criminal behaviour) which have, in effect, become private again, for example through the passage of time. Nevertheless, the public disclosure of public facts will have to be highly offensive to an objective reasonable person.

(3) (a) It is inconsistent with an individual's privacy to allow the public disclosure of material obtained by intentionally interfering, in the nature of prying, with that individual's interest in solitude or seclusion. The intrusion must be highly offensive to an objective reasonable person.

249 Broadcasting Act 1989, s 4(1)(c).

250 Broadcasting Act 1989, s 6.

251 Broadcasting Act 1989, s 7.

252 Broadcasting Act 1989, s 8(1A).

253 *TV3 Network Services Ltd v Broadcasting Standards Authority* [1995] 2 NZLR 720.

254 Broadcasting Standards Authority "Privacy Principles" www.bsa.govt.nz (accessed 10 March 2008).

(b) In general, an individual's interest in solitude or seclusion does not prohibit recording, filming, or photographing that individual in a public place ("the public place exemption").

(c) The public place exemption does not apply when the individual whose privacy has allegedly been infringed was particularly vulnerable, and where the disclosure is highly offensive to an objective reasonable person.

(4) The protection of privacy includes the protection against the disclosure by the broadcaster, without consent, of the name and/or address and/or telephone number of an identifiable individual, in circumstances where the disclosure is highly offensive to an objective reasonable person.

(5) It is a defence to a privacy complaint that the individual whose privacy is allegedly infringed by the disclosure complained about gave his or her informed consent to the disclosure. A guardian of a child can consent on behalf of that child.

(6) Children's vulnerability must be a prime concern to broadcasters, even when informed consent has been obtained. Where a broadcast breaches a child's privacy, broadcasters shall satisfy themselves that the broadcast is in the child's best interests, regardless of whether consent has been obtained.

(7) For the purpose of these Principles only, a "child" is defined as someone under the age of 16 years. An individual aged 16 years or over can consent to broadcasts that would otherwise breach their privacy.

(8) Disclosing the matter in the "public interest", defined as of legitimate concern or interest to the public, is a defence to a privacy complaint.

3.40 Generally there is no formal hearing, but the BSA must give the complainant and the broadcaster a reasonable opportunity to make written submissions.[255] If the BSA decides that the complaint is justified in whole or in part, it may make orders:

- directing the broadcaster to publish a statement relating to the complaint;
- directing the broadcaster to refrain from broadcasting, or from broadcasting advertising programmes, for a period not exceeding 24 hours;
- referring the complaint back to the broadcaster for consideration and determination by the broadcaster in accordance with such directions or guidelines as the BSA thinks fit;
- requiring the broadcaster to pay costs of up to $5000 to the Crown; or,
- where the BSA finds that the broadcaster has failed to maintain privacy standards, directing the broadcaster to pay compensation not exceeding $5000.[256]

3.41 The BSA has received an average of around 160 complaints per year over the past five years. Less than ten per cent of these related to the privacy standard.[257] Approximately one quarter of complaints are upheld. In about half of these cases, simply upholding the complaint will be regarded as sufficient penalty. Where a remedy is awarded, most commonly the BSA will order the broadcast of a statement summarising its decision. This tends to occur where there has been a serious breach, injury to someone depicted, fault on the part of the broadcaster or a high public interest. An apology may be ordered where a person or organisation has been badly harmed by the breach of privacy. In particularly

255 Broadcasting Act 1989, s 10.

256 Broadcasting Act 1989, ss 13, 16(4).

257 Broadcasting Standards Authority *Annual Report 2006-2007* (Wellington, 2007).

serious cases, the BSA may order that the media organisation broadcast an apology via other forms of media, such as taking out advertisements in newspapers. The BSA rarely imposes the more severe sanctions available to it, such as ordering a broadcaster off air or ordering that compensation be paid.[258]

BSA approach to privacy

3.42 BSA decisions have not always been consistent. However, it has developed quite a significant privacy jurisprudence, from which it is possible to discern patterns.

3.43 The most common privacy complaint is the publication of private facts. The BSA has defined private facts as material that gives rise to an expectation of privacy. It must be in some way personal and sensitive or intimate, and not already in the public domain. However, it may include facts that are known to some extent by others. For example, if a fact has earlier been publicised, it may become private again depending on the significance of the fact and the extent to which it was publicised.[259] Furthermore, events that occur in a public place have not usually been treated as private facts. Therefore, the BSA has generally found that filming people in a public place, even without their consent, is not a breach of privacy.[260]

3.44 A disclosure of private facts must be highly offensive to an objective reasonable person. The BSA has generally found disclosures to be highly offensive where, for example, the material is very embarrassing, sensitive or traumatic, the subject clearly did not want to be filmed or recorded, the subject is particularly vulnerable, or the publicity did not advance understanding of a matter of public interest.[261]

3.45 Even where a disclosure is found to be highly offensive, it may be allowed in the public interest. The BSA has developed guidance as to what is in the public interest. It includes:

- criminal matters, including exposing or detecting crime;
- issues of public health or safety;
- matters of politics, government or public administration;
- matters relating to the conduct of organisations which impact on the public;
- exposing misleading claims made by individuals or organisations;
- exposing seriously anti-social or harmful conduct; and
- other things of importance or concern to the New Zealand public generally.[262]

It is not enough that a programme is generally in the public interest. The particular material must also be in the public interest.

---

258 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 5-6.

259 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 109-111.

260 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 112.

261 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 113-114.

262 *Balfour v TVNZ* (21 March 2006) Broadcasting Standards Authority 2005-129.

3.46 The BSA also has an intrusion principle, which need not involve revealing private facts. It is concerned with how information is collected. The principle applies when a person is filmed, recorded or spied on when he or she could reasonably expect to be left alone. The intrusion must be highly offensive to an objective reasonable person. The BSA is especially likely to find that there has been an intrusion where the person is at home or in another private place, does not know about the filming or recording, has been in some way deceived about the filming or recording or its purpose, or has made clear efforts to escape public or media attention. The intrusion standard may be breached by means other than prying; for example, by victimisation or exploitation of subjects. It will generally not be an intrusion to film people in public places.[263]

3.47 The BSA standards on Fairness are also relevant to some privacy-intrusive activities such as covert visual or audio recording.[264]

Press Council

3.48 The Press Council is a voluntary industry body established to provide a forum for resolution of complaints against newspapers and magazines (including their websites). Given its voluntary nature, it does not fully cover all print media, and does not have any legal powers.[265] The Council is strongly committed to promoting freedom of the press and freedom of expression.

3.49 The Council has established a set of principles, which are not intended as a code, but may be used by complainants in order to describe the nature of their complaint. Its privacy principle states that:[266]

> [e]veryone is entitled to privacy of person, space and personal information, and these rights should be respected by publications. Nevertheless the right of privacy should not interfere with publication of matters of public record, or obvious significant public interest.
>
> Publications should exercise care and discretion before identifying relatives of persons convicted or accused of crime where the reference to them is not directly relevant to the matter reported.
>
> Those suffering from trauma or grief call for special consideration, and when approached, or enquiries are being undertaken, careful attention is to be given to their sensibilities.

3.50 Individuals who believe that these standards have been breached must first complain in writing to the editor of the relevant publication, within three months of the date of publication of the material to which the complaint relates.

263 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 117-119.

264 See discussion in chapter 12 below.

265 John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, Melbourne, 2005) 576, 620.

266 Press Council "Statement of Principles", Principle 3, www.presscouncil.org.nz (accessed 10 March 2008).

3.51 Complainants who are not satisfied with the response from the editor, or have not received a reply within a reasonable period of time, can then write to the Council detailing the nature of the complaint, giving precise details of the publication in which the relevant material was published, and enclosing copies of correspondence with the editor, the material that is the subject of the complaint and any other relevant evidence.

3.52 The Council then copies the complaint to the editor, who is given 14 days in which to respond. Upon receiving the editor's response, the complainant is given 14 days in which to comment to the Council on the response. The complainant does not need to do this if satisfied with the response. The editor is then given a further 14 days in which to make a final response.

3.53 The Council will then conduct an adjudication. This occurs at a meeting of the Council, where the Council considers the complaint file. The results are communicated to the parties. If the Council upholds the complaint in full or in part, the publication concerned must publish the essence of the decision, giving it fair prominence.[267]

3.54 In circumstances where a legally-actionable issue may be involved, the complainant is required to provide a written undertaking not to take or continue proceedings against the publication or journalist concerned. This is intended to prevent the Press Council being used as a test forum for litigation.

3.55 The Press Council has usually received 75 or more complaints per year since 2000.[268] It has upheld around 22 per cent of complaints over the past five years, although this proportion seems to be rising.[269] Fairly frequently, its decisions identify ethical shortcomings but conclude that they are not serious enough to uphold the complaint.

3.56 In 2007 an independent review of the Press Council was carried out. It concluded that the Council has generally performed usefully, but recommended some changes to its operation.[270] These recommendations have not yet been implemented.

Press Council approach to privacy

3.57 The Press Council has not generally discussed the general principles underlying its privacy standard, although it is likely that it would consider similar matters to those that the courts and the BSA consider. These would include matters such

267 Press Council "Complaints Procedure" www.presscouncil.org.nz (accessed 10 March 2008).

268 See statistics in Ian Barker and Lewis Evans *Review of the New Zealand Press Council* (New Zealand Press Council, Wellington, 2007) 52; New Zealand Press Council *Annual Report 2007* (Wellington, 2008) 37.

269 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 153.

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

as whether there was a reasonable expectation of privacy, whether private or sensitive facts were revealed, and whether the disclosure was highly offensive to an objective reasonable person.[271]

3.58 The Press Council will generally uphold a privacy complaint where sensitive facts are published about an identifiable person who could reasonably expect those facts to be kept private. In terms of identification, the Press Council asks whether there was sufficient material to enable the public to identify the complainant. It will sometimes be enough that the material enabled family and friends to identify the complainant.[272]

3.59 Complaints will not generally be upheld where photographs are taken in public places, the information is in the public domain, the information relates to the public lives of public figures, or the material is of public interest. Publishing the names of people involved in newsworthy events or addresses and photographs of homes or businesses involved in such events will also generally not be found to breach privacy. Particular care is required in dealing with children and victims of crimes and accidents.[273]

3.60 Publication of private facts can be justified where there is public interest in the material. The Press Council has not defined public interest, but has listed some things which will be in the public interest. These are:

- political coverage;
- the use of public money; and
- exposing deception or hypocrisy.[274]

3.61 The review of the Press Council reported that some submissions had said that the Council's Principles need to be more specific on privacy. The reviewers noted that the Australian Press Council's guidelines on privacy were worthy of consideration, and that codification of privacy standards for the print media might assist in preserving the media exclusion from the Privacy Act. They recommended that the Press Council undertake an immediate review of its current Principles.[275]

Advertising Standards Authority

3.62 The Advertising Standards Authority (ASA) is a voluntary industry body established to maintain advertising standards and deal with complaints about advertisements. It has established Advertising Codes of Practice setting out standards relating to particular types of advertising.

271 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 195.

272 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 196.

273 Steven Price "Complaints Against the Media" in *Media Law – Rapid Change, Recent Developments* (New Zealand Law Society, 2008) 63, 74.

274 Steven Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 198.

275 Ian Barker and Lewis Evans *Review of the New Zealand Press Council* (New Zealand Press Council, Wellington, 2007) 73.

3.63 Privacy is covered only briefly in the ASA's Advertising Code of Ethics. The relevant rule provides that:[276]

> [u]nless prior permission has been obtained an advertisement should not portray or refer to any persons, whether in a private or public capacity, or refer to any person's property, in a way likely to convey the impression of a genuine endorsement.

3.64 Any person may complain to the ASA about an advertisement in any media that they believe breaches a Code. The ASA has established a separate body, the Advertising Standards Complaints Board, to consider and determine complaints. Complaints must be directed to this body. Upon receiving a complaint, the Chairperson will determine whether the complaint is suitable to be considered by the Board and is within the Board's jurisdiction. If so, the complaint will be sent to the advertiser, the advertising agency and relevant media, seeking their opinion and comments.

3.65 After considering the responses, the Board will then determine whether there has been a breach of the relevant Code(s) of Practice and inform all parties of the outcome. If a complaint is upheld, the advertiser is requested to voluntarily and immediately withdraw the advertisement. The media are also requested not to publish or broadcast the advertisement. Advertisers and the media comply with these requests.

3.66 There is also an Advertising Standards Complaints Appeal Board, which may hear appeals on certain limited grounds.[277]

3.67 In 2007 the Advertising Standards Complaints Board received 1160 complaints about 668 advertisements. Of these, a number were duplicates or were deemed to have no grounds to proceed. Therefore, the Board considered complaints about 313 advertisements. Of these, 109 were upheld, 68 were settled and 135 were not upheld. The number of complaints upheld was relatively similar to the ten preceding years.[278] It appears that most complaints did not relate to privacy.[279]

OTHER INDUSTRY COMPLAINTS MECHANISMS

Marketing Association

3.68 The New Zealand Marketing Association has established a Code of Practice for Direct Marketing in New Zealand.[280] The Code requires that consumers must be able to opt out from receiving marketing information that they have not requested, and marketers must have systems in place to enable them to honour requests to opt out. Consumers must also be given notice if they are being recorded. The Association has a complaints process if marketers do not comply with the code.

276 Advertising Standards Authority "Advertising Code of Ethics"; see also "Code for Advertising to Children", Guideline 4(c) www.asa.co.nz (accessed 2 December 2008).

277 Advertising Standards Authority "How to Make a Complaint" www.asa.co.nz (accessed 16 May 2008).

278 Advertising Standards Authority *Annual Report 2007* (Wellington, 2007) 21.

279 Advertising Standards Authority *Annual Report 2007* (Wellington, 2007) 25.

280 New Zealand Marketing Association "Code of Practice for Direct Marketing in New Zealand" www.marketing.org.nz (accessed 11 December 2008).

Market Research Society

3.69 The Code of Practice of the Market Research Society of New Zealand contains a number of provisions relevant to privacy. In particular, article 7 deals with data protection and privacy, and contains a number of standards relating to the collection and use of data, security of processing, transborder transactions and the rights of those participating in market research.[281] The Code also requires that people be given notice if they are being recorded.

3.70 People can complain to the Market Research Society of New Zealand if they believe that a member has breached the Code. Upon receipt of a complaint, the Society appoints a complaints officer, who investigates and tries to resolve the complaint, and reports to the President of the Society. Following this report, a complaints committee is set up to consider the Complaints Officer's report and try to resolve the complaint. If the committee is unable to resolve the complaint, and it considers that it has sufficient substance, it can refer it to the Market Research Society Committee, which may take action against the member that was the subject of the complaint, including reprimanding the member, requiring the member to make good the breach and suspending or expelling the member from the Society.[282]

UNSOLICITED ELECTRONIC MESSAGES ACT 2007

3.71 The Unsolicited Electronic Messages Act 2007 may also be considered part of the regulatory framework for privacy. It prohibits sending unsolicited commercial electronic messages ("spam"), requires commercial electronic messages to include accurate sender information and a functional unsubscribe facility, and restricts the use of address-harvesting software and harvested address lists. There is provision for pecuniary penalties, compensation and damages for breach of the Act. The Act is enforced by an enforcement department, although the Courts also have significant powers in the case of serious transgressions.

281 Market Research New Zealand "Code of Practice 2008" www.mrsnz.org.nz/Resources/Code-of-Practice-2008.asp (accessed 15 December 2008).

282 Market Research New Zealand "Complaints Procedure" www.mrsnz.org.nz/Contact-Us/Complaints-Procedure.asp (accessed 15 December 2008).

Chapter 4
Other jurisdictions

4.1 New Zealand privacy law has features in common with the privacy law of other comparable jurisdictions, and has been influenced by models and jurisprudence from overseas to some extent. In this chapter we focus on the privacy law of the United States, Europe as a whole, the United Kingdom, the Republic of Ireland, Australia and Canada. Most of these jurisdictions have some kind of personal information protection law equivalent to New Zealand's Privacy Act 1993; laws criminalising certain types of surveillance and other privacy-intrusive activities; and some system for regulating privacy standards in the media. Some jurisdictions also recognise a right to privacy that is enforceable in the courts, but the source of this right varies: it may be found in common law, statute, human rights charters, constitutions, or some combination of these. After surveying the situation in these other jurisdictions in this chapter, we consider what New Zealand may be able to learn from the experience overseas in chapter 5.

UNITED STATES

4.2 The United States has a large number of state and Federal statutes covering particular aspects of privacy. Perhaps the most notable features of privacy law in the United States are the torts of invasion of privacy. It is now more than a century since United States courts began recognising some form of common-law privacy tort, and some states also have statutory torts. Despite this, the volume of privacy cases is not large, and plaintiffs are often unsuccessful. The tort of public disclosure of private facts, in particular, has been severely limited by the constitutional protection of freedom of speech.

Constitutional protection of privacy

4.3 There is no express right to privacy in the United States Constitution, although it is explicitly protected in some state constitutions.[283] The Fourth Amendment to the US Constitution protects against unreasonable searches and seizures, and provides that warrants shall not be issued without probable cause. The decision of the United States Supreme Court in *Katz v United States* held that Fourth Amendment protections apply in situations in which a person has a reasonable expectation of privacy.[284] This reversed the Court's previous approach, which had limited the Fourth Amendment's coverage to physical

283 Daniel Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2004) 62.

284 *Katz v United States* (1967) 389 US 347.

intrusions by authorities into "constitutionally-protected areas" such as homes. As a result of *Katz*, Fourth Amendment protections were extended to wiretapping and other forms of electronic eavesdropping.

4.4 It can be argued that some of the other amendments that make up the Bill of Rights also implicitly protect privacy,[285] and this argument has been accepted by the United States Supreme Court.[286] In *Griswold v Connecticut*,[287] the Court held that "penumbras" associated with a number of rights guaranteed in the Bill of Rights formed constitutionally-protected "zones of privacy". *Griswold* was concerned with access to contraception, and the "privacy" in question was the right to be free from state interference in decisions concerning intimate, personal matters. The Court subsequently extended this protection to other areas, such as abortion.[288] Matters such as these would not usually be considered in terms of privacy in New Zealand. The United States Supreme Court has recognised that, in addition to protecting decisional privacy, the constitutional privacy cases protect "the individual interest in avoiding disclosure of personal matters".[289] The constitutional protection against disclosure of personal matters appears to be fairly narrow, however, and like all constitutional rights it applies only to action by the state.[290]

4.5 The First Amendment's protection of freedom of assembly is one of the constitutional guarantees that has been cited as carving out a "zone of privacy".[291] However, as we discuss below, First Amendment rights to freedom of speech and of the press have often been in tension with the protection of privacy.

Tort

4.6 The United States has a significant body of tort law relating to invasion of privacy, which has been influential in other countries, including New Zealand. The Court of Appeal in *Hosking v Runting* cited the United States jurisprudence, and the *Hosking* tort is clearly modelled on the US tort of public disclosure of private facts.[292] The Broadcasting Standards Authority also looked to the

285 Daniel Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2004) 62-64.

286 For further discussion of the Supreme Court's privacy jurisprudence, see Sanford Levinson "Privacy" in Kermit L Hall (ed) *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press, New York, 1992) 671.

287 (1965) 381 US 479.

288 *Roe v Wade* (1972) 410 US 113.

289 *Whalen v Roe* (1977) 429 US 589, 599.

290 Daniel J Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2004) 65-67; "Privacy After Roe: Informational Privacy, Privacy of the Home or Personal Autonomy?" in Johnny H Killian, George A Costello and Kenneth R Thomas (eds) *Analysis and Interpretation of the Constitution* (Congressional Research Service, Library of Congress, 2002 [updated 2004]), accessed online at http://supreme.justia.com/constitution (accessed 18 July 2008).

291 Daniel J Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2004) 62-63.

292 *Hosking v Runting* [2005] 1 NZLR 1, paras 66-76, 117-118 (CA) Gault P and Blanchard J.

United States when developing its privacy principles, and those principles draw heavily on the US torts of disclosure of private facts and intrusion into seclusion.[293]

4.7 United States privacy tort law originated with an 1890 article on "The Right to Privacy" by Samuel Warren and Louis Brandeis.[294] Concerned about what they saw as increasing intrusions into privacy by the popular press, Warren and Brandeis argued that various strands in the existing common law could form the basis for a previously-unrecognised legal right to privacy. The remedies for invasions of privacy would be "An action of tort for damages in all cases" and "An injunction, in perhaps a very limited class of cases". They also suggested that privacy should receive additional protection from the criminal law.[295]

4.8 Although the courts in the United States did not immediately accept the argument put forward by Warren and Brandeis, the tort of invasion of privacy gradually gained recognition in most US states. Today, almost all states recognise a common-law tort of invasion of privacy, and some states have created a statutory cause of action for one or more of the privacy torts discussed below.[296] Arguably as important in the development of the tort as the original Warren and Brandeis article was a 1960 article by William Prosser, based on a survey of over 300 cases decided by that time.[297] Prosser concluded that there were in fact four distinct privacy torts:

- intrusion upon seclusion;
- public disclosure of private facts;
- publicity which places the plaintiff in a false light in the public eye; and
- appropriation of the plaintiff's name or likeness.

Prosser's classification of the torts was subsequently adopted by the American Law Institute's Restatements of the Law.[298] Most states follow the formulation of the tort set out in the *Restatement*, but there are jurisdictional differences and some states depart in certain respects from the general principles set out in the *Restatement*.[299]

4.9 Prosser did not include breach of confidentiality in his classification of the tort of invasion of privacy, and the confidentiality tort has been relatively undeveloped in the United States in comparison with the privacy torts. It has remained largely restricted to cases involving some form of contractual or professional relationship

293 Michael Stace *Privacy: Interpreting the Broadcasting Standards Authority's Decisions January 1990 to June 1998* (Dunmore Press/Broadcasting Standards Authority, Palmerston North, 1998) 17-18.

294 Samuel D Warren and Louis Brandeis "The Right to Privacy" (1890) 4 Harv L Rev 193.

295 Samuel D Warren and Louis Brandeis "The Right to Privacy" (1890) 4 Harv L Rev 193, 219.

296 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 93-95.

297 William L Prosser "Privacy" (1960) 48 Cal L Rev 383.

298 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652.

299 Neil M Richards and Daniel J Solove "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Geo LJ 123, 153; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 95.

between the parties, especially doctor-patient relationships.[300] This stands in contrast to English law, which has recognised privacy largely by adapting the well-developed existing law on breach of confidentiality.

General principles

4.10 According to the *Restatement of the Law of Torts*, the following principles apply to the four privacy torts generally:[301]

- Where a plaintiff brings an action on grounds that relate to two or more of the privacy torts, he or she may have only one recovery of damages for invasion of privacy.
- The rules on absolute and conditional privileges to publish defamatory matter apply also to publication of matter that is an invasion of privacy.
- Damages may be recovered for harm caused by the invasion, mental distress, and any special damage.
- An action for invasion of privacy is a personal right, which can be maintained only by a living person whose privacy has been invaded. In general, the action lapses on death. It cannot be brought by persons other than the person who has suffered the invasion, or by corporations, partnerships or unincorporated associations.[302]

Intrusion upon seclusion

4.11 Liability for invasion of privacy exists where a person "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his [or her] private affairs or concerns, … if the intrusion would be highly offensive to a reasonable person".[303] The invasion could involve a physical intrusion into a place where the plaintiff expects to be left undisturbed; the use of the defendant's senses to oversee or overhear the plaintiff's private affairs (including the use of devices to aid the senses, such as wiretaps, microphones or cameras); or other intrusions such as opening sealed mail, rifling through a person's wallet, or unauthorised examination of a private bank account. No publication or use of the information obtained, or publicity of the plaintiff's private affairs, is required for this tort: the invasion consists of the intentional intrusion itself.

4.12 For an intrusion to take place, the plaintiff must have a reasonable expectation of privacy: the intrusion must be into a private place, conversation or matter. There is no liability for examination of matters that are on the public record, or, in most cases, for observing or photographing a person in a public place. However, there are some circumstances in which there can be an intrusion into

300 Neil M Richards and Daniel J Solove "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Geo LJ 123, 151-153, 156-158; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 96-97.

301 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) §§ 652A, 652F, 652G, 652H, 652I.

302 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652I; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 95-96, 113-114. There are some exceptions to these general rules in the case law and in some statutes, particularly in relation to the tort of appropriation of name or likeness.

303 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652B; see also New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 106-111.

private matters even in a public place; for example, in the often-cited case of a woman who is photographed when her dress is unexpectedly blown up by an air jet, revealing her underwear.[304] The defendant is not liable unless the interference with seclusion is substantial, such that it would be considered highly offensive by an ordinary reasonable person. So, for example, it would not be an invasion of privacy to knock on someone's door or to call a person on the phone once or twice, but persistent hounding of a person could be an invasion.

Public disclosure of private facts

4.13 A person's privacy may be invaded when private facts about him or her are publicly disclosed, if the matter disclosed is of a kind that would be highly offensive to a reasonable person and is not of legitimate concern to the public.[305] In general, public disclosure or publicity means that the matter is communicated to the public at large or to a substantial body of persons, but the size of the audience required will depend on the particular facts of the case. In some cases, disclosure to a small number of individuals with whom the plaintiff has a special relationship may satisfy the publicity requirement. As with the intrusion tort, there will generally be no liability when the matter disclosed is already well known, is on the public record, or occurred in a public place.

4.14 Publicity given to private facts is not an invasion of privacy unless it would be considered highly offensive to an ordinary, reasonable person. The *Restatement* notes that the protection of privacy will be relative to local customs and habits, and that reporting of ordinary daily activities will not give the plaintiff a cause of action under the publicity tort: the cause of action only arises when "a reasonable person would feel justified in feeling seriously aggrieved" by the publicity.[306] So, publicity given to matters such as sexual activity or sexual abuse may be offensive to a reasonable person, whereas publication of facts that are merely unflattering, mildly embarrassing or annoying will not be considered an invasion of privacy. Furthermore, even if a matter that is publicised would be highly offensive, there may be no invasion of privacy if it is a matter of legitimate public concern (although whether the public interest principle is a defence or an element of the tort varies between jurisdictions).

False light

4.15 Publicising "a matter concerning another that places the other before the public in a false light", where the actor knows or is reckless as to the falsity of the matter and the false light in which the other would be placed, and where the false light in which the other was placed would be highly offensive to a reasonable person, is an invasion of privacy.[307] Again, publicity is required, but in the case of the false-light tort the matter publicised must be false. However, there have been cases in which the courts have found that a person has been put in a false light by the publication of statements that, while technically

304 *Daily Times Democrat v Graham* (1964) 276 Ala 380.

305 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652D; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 99-106.

306 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652D, comment c.

307 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652E; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 115-120.

true, create a false impression in the absence of other explanatory facts and circumstances. The plaintiff must also show that the false statements are understood to be about him or her, and cannot reasonably be construed as referring to someone else. Minor inaccuracies or unimportant false statements will not usually be an invasion of privacy: there must be such a major misrepresentation of a person's "character, history, activities or beliefs that serious offense may reasonably be expected to be taken" by a reasonable person in the position of the plaintiff.[308]

4.16 The false-light tort is clearly closely related to defamation, but the two actions differ in several ways:[309]

- The false-light tort is not restricted to publicity of matters that would be considered defamatory.
- A defamation action can be based on publication of a matter to a single person, whereas the false-light tort generally requires a matter to be publicised to a substantial section of the public.
- Defamation is based on injury to reputation, while the false-light tort is primarily intended to provide remedies for humiliation, embarrassment and other forms of mental distress.

Nonetheless, the considerable area of overlap between the two causes of action has troubled some commentators, who consider that the false-light tort deals with matters that are more properly part of the law of defamation.[310] It is possible to bring an action for both defamation and false-light invasion of privacy, although only one recovery of damages can be had.

Appropriation

4.17 The fourth of the United States privacy torts involves liability for invasion of privacy where a person appropriates the name or likeness of another for the defendant's own purpose or benefit.[311] In essence, what is protected by this tort is the plaintiff's identity. The invasion could take a number of forms, including using a photograph of the plaintiff in an advertisement, or posing as or impersonating the plaintiff. In many cases the appropriation will be for the defendant's commercial benefit, such as advertising the defendant's products or services, although the common-law tort is not restricted to commercial appropriation.[312] Mere use of the same name as the plaintiff is not an invasion of privacy unless the plaintiff attempts to pass himself or herself off as the plaintiff, or to appropriate the value of the name (that is, the plaintiff's reputation or social or commercial standing). Nor is merely incidental use, such as mentioning the plaintiff's name or using the plaintiff's image in a news story, an appropriation.

308 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652E, comment c.

309 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 119-120.

310 Harry Kalven, Jr "Privacy in Tort Law – Were Warren and Brandeis Wrong?" (1966) 31 Law & Contemp Probs 326, 339-341; Raymond Wacks "The Poverty of 'Privacy'" (1980) 96 LQR 73, 83-85.

311 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652C; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 111-115.

312 Statutes in some states do restrict the tort to commercial appropriation.

4.18 While the appropriation tort protects the plaintiff's dignitary interests, and provides a remedy for mental distress, it can also be viewed as protecting something in the nature of a property right. To the extent that it recognises a property right, it may be alienable and may also survive death, a point on which the courts have been divided. Some jurisdictions have gone further, recognising a "right of publicity" which gives celebrities exclusive rights to the use of their names and likenesses. The right of publicity is clearly a property right, and survives death.[313]

The privacy torts and the First Amendment

4.19 The First Amendment to the United States Constitution guarantees the rights of freedom of speech and freedom of the press, among other rights. These guarantees have implications for all four of the privacy torts, but especially for the tort of disclosure of private facts. While the death of that tort has been predicted,[314] it and the other privacy torts have "by and large survived the First Amendment challenges and remain viable torts, even though they are infrequently invoked."[315] The United States Supreme Court has never held that the privacy torts are unconstitutional. The Court has favoured an approach of balancing free speech against other important interests, and case law currently holds that some forms of speech (such as commercial speech) require less protection than others. It is arguable that speech of private concern warrants less protection under the First Amendment than speech of public concern, leaving room for restrictions on truthful speech in some cases.[316]

4.20 Nonetheless, freedom of speech and of the press weigh very heavily in any balancing exercise, and publicity given to matters of legitimate public concern will not be an invasion of privacy.[317] In *Florida Star v BJF*,[318] which concerned the publication of the name of a rape victim, the United States Supreme Court held that the award of damages against the defendant newspaper violated the First Amendment, but noted that:[319]

> We do not hold that truthful publication is automatically constitutionally protected, or that there is no zone of personal privacy within which the State may protect the

313 For further discussion see Huw Beverley-Smith *The Commercial Appropriation of Personality* (Cambridge University Press, Cambridge, 2002).

314 See for example Diane L Zimmermann "Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort" (1983) 68 Cornell L Rev 291.

315 Neil M Richards and Daniel J Solove "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Geo LJ 123, 155.

316 Daniel J Solove "The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure" (2003) 53 Duke LJ 967, 977-989; Daniel J Solove *The Future of Reputation: Gossip, Rumour and Privacy on the Internet* (Yale University Press, New Haven, 2007) 127-129; Fred H Cate and Robert Litan "Constitutional Issues in Informational Privacy" (2002) 9 Mich Telecomm Tech L Rev 35, 49-53. See also Patrick M Garry "Commercial Speech", Henry J Abraham "First Amendment Absolutism" and "First Amendment Balancing", and Bill F Chamberlin "Speech and the Press", in Kermit L Hall (ed) *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press, New York, 1992) 169, 299, 300, 808.

317 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652D, comment d. In some United States jurisdictions legitimate public concern is an element of the tort, while in others it is a defence.

318 *Florida Star v BJF* (1989) 491 US 524.

319 *Florida Star v BJF* (1989) 491 US 524, 541 Marshall J.

> individual from intrusion by the press, or even that the State may never punish publication of the name of a victim of a sexual offense. We hold only that, where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order…

In a significant dissent, Justice White stated that the Court's ruling against the plaintiff threatened "to obliterate one of the most notable legal inventions of the 20th century: the tort of the publication of private facts". If the First Amendment prevented a private person from recovering for publication of the fact that she had been raped, it was doubtful whether there were any private facts which a person could assume would not be published or broadcast.[320]

4.21 The First Amendment issues concerning the other privacy torts are somewhat different from those relating to the disclosure tort. In the case of the intrusion tort, the United States Supreme Court has not generally afforded the same degree of protection to the gathering of information by the news media as it has to the media's publication of information.[321] The California Supreme Court has also drawn a distinction between the way in which the First Amendment affected a plaintiff's claims under the intrusion and disclosure torts:[322]

> [T]he constitutional protection accorded newsgathering, if any, is far narrower than the protection surrounding the publication of truthful material… The reason for the difference is simple: The intrusion tort, unlike that for publication of private facts, does not subject the press to liability for the contents of its publications…. [N]o constitutional precedent or principle of which we are aware gives a reporter general license to intrude in an objectively offensive manner into private places, conversations or matters merely because the reporter thinks he or she may thereby find something that will warrant publication or broadcast.

4.22 There are two main ways in which the courts have limited the scope of the false-light tort to ensure that it is consistent with the First Amendment. First, some cases have decided that media defendants cannot be held liable for false-light invasion of privacy merely on the grounds that they failed to include additional facts that might have portrayed the defendant in a more favourable light.[323] Secondly, the United States Supreme Court in *Time, Inc v Hill* held that it would be a violation of the First Amendment to allow redress for "false reports of matters of public interest in the absence of proof that the defendant published the report with knowledge of its falsity or in reckless disregard of the truth."[324]

---

320 *Florida Star v BJF* (1989) 491 US 524, 550-551 White J. White J was joined in his dissent by Rehnquist CJ and O'Connor J.

321 Bill F Chamberlin "Speech and the Press" in Kermit L Hall (ed) *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press, New York, 1992) 808, 813.

322 *Schulman v Group W Productions, Inc* (1998) 955 P 2d 469, 496-497 (Cal Supreme Court) Werdegar J.

323 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 117-118. However, as noted above, there are other cases in which defendants have been held liable for publishing facts that, while true, create a misleading impression in the absence of other facts.

324 *Time, Inc v Hill* (1967) 385 US 374, 397-388 Brennan J. This application of the "actual malice" standard (borrowed from the defamation case of *New York Times Co v Sullivan* (1964) 376 US 254) has been called into question by a later Supreme Court ruling that, in a defamation claim, a private figure need only prove some "fault" (such as negligence): *Gertz v Robert Welch, Inc* (1974) 418 US 323.

4.23 In appropriation cases, the tort cannot be maintained where the appropriation of the plaintiff's name or likeness occurs through the publication of material that is newsworthy or of public concern. However, commercial speech is less likely to raise free speech concerns than other forms of speech.[325] The United States Supreme Court has upheld a state law providing for the "right of publicity" branch of the appropriation tort, since it protected a proprietary interest rather than feelings or reputation, and would not prevent the reporting of newsworthy facts.[326]

4.24 Finally, it should be noted that the jurisprudence discussed above relates to the publication or broadcast of material by the media. The question of whether commercial uses of personal information not involving publication or public expression can be restricted consistently with the First Amendment has not yet been decided by the United States Supreme Court.[327]

Conclusion

4.25 While the First Amendment right of freedom of speech has not eliminated the United States privacy torts, it has limited them, quite severely so in the case of the public disclosure tort. This led Gault P and Blanchard J in *Hosking v Runting* to observe that "the right to privacy in the United States [seems] a somewhat hollow one".[328] The volume of cases is relatively low, and plaintiffs in public disclosure cases are seldom successful.[329] Despite this, the United States experience illustrates the issues with which the *Hosking* tort or any new statutory tort might have to deal and the principles developed there may assist with the development of our own privacy law.[330] However, the different constitutional framework and social climate must be kept in mind when drawing lessons from the United States jurisprudence.

Privacy legislation

4.26 The United States stands out among developed countries for the fact that it has no comprehensive privacy law, and no national authority with primary responsibility for protecting privacy.[331] The Privacy Act of 1974 was a pioneering

325 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 114-115.

326 *Zacchini v Scripps-Howard Broadcasting Co* (1977) 433 US 562, 573-574 White J.

327 Fred H Cate and Robert Litan "Constitutional Issues in Informational Privacy" (2002) 9 Mich Telecomm Tech L Rev 35, 54-56.

328 *Hosking v Runting* [2005] 1 NZLR 1, para 73 (CA).

329 Randall Bezanson reports that a survey of public disclosure privacy cases brought to trial showed that plaintiffs win fewer than 3 per cent of cases: "The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990" (1992) 80 Cal L Rev 1133, 1172 (n 115). See also Diane L Zimmermann "Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort" (1983) 68 Cornell L Rev 291, 293 (n 5).

330 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 121-122.

331 For some summaries of Federal privacy statutes in the United States, see Albert Marcella and Carol Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (John Wiley & Sons, Hoboken (NJ), 2003), ch 5; Daniel Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2004) 67-73; Avner Levin and Mary Jo Nicholson "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground" (2005) 2 UOLTJ 357, 362-374.

piece of privacy legislation, but it applies only to the Federal government.[332] Instead of national legislation broadly covering the public and private sectors, there are a large number of privacy laws at both Federal and state levels covering particular issues or sectors. Federal laws include those concerning credit reporting,[333] student records,[334] electronic surveillance by government,[335] motor vehicle records,[336] health information,[337] and collection of children's personal information online.[338] A number of pieces of privacy-protective legislation were amended by the USA PATRIOT Act of 2001,[339] which gave greater powers to law enforcement agencies in the wake of the 11 September 2001 terrorist attacks in the United States. Another source of privacy protection is the Federal Trade Commission's power to bring actions against companies for unfair or deceptive practices. This allows the Commission to take enforcement action against companies that break their own privacy policies.

4.27 The criminal laws relating to privacy are too various to summarise here. For example, the California Penal Code has provisions on invasion of privacy which create offences relating, among other things, to interception of and eavesdropping on private conversations, and use of electronic tracking devices.[340]

Regulation of the media

4.28 There is no government agency in the United States with responsibility for enforcing privacy standards in the media, and any attempt by the government to mandate such standards would undoubtedly be held to be unconstitutional on First Amendment grounds. The Federal Communications Commission (FCC) is responsible for regulation of radio and television broadcasting, but has only a very limited role in regulating content. The only area of regulation by the FCC that relates to privacy involves restrictions on the broadcast of telephone conversations if any party to the conversation has not been informed that it is to be broadcast.[341] There is no national body responsible for regulating the press. Instead, many newspapers have their own ombudsmen, to whom complaints can be made.[342] A few states have press councils established by the newspaper industry as self-regulatory bodies, like the New Zealand Press Council.[343]

---

332 Privacy Act of 1974 5 USC § 552a.

333 Fair Credit Reporting Act of 1970 15 USC § 1681.

334 Family Educational Rights and Privacy Act of 1974 20 USC § 1232g.

335 Electronic Communications Privacy Act of 1986 18 USC §§ 2510-2522; 2701-2710.

336 Driver's Privacy Protection Act of 1994 18 USC § 2721.

337 Health Insurance Portability and Accountability Act of 1996 Pub L No 104-191, 110 Stat 1936 (1996).

338 Children's Online Privacy Protection Act of 1998 15 USC § 6501-6506.

339 USA PATRIOT Act of 2001 Pub L No 107-56 115 Stat 272 (2001).

340 California Penal Code §§ 630-638. For a summary of state laws on surreptitious recording and use of hidden cameras see Reporters Committee for Freedom of the Press *The First Amendment Handbook* (Arlington, VA, 2003) ch 3, available at www.rcfp.org.

341 *The Public and Broadcasting: How to Get the Most from Your Local Station* (Media Bureau, Federal Communications Commission, Washington, DC, 2008).

342 See the website of the Organization of Newspaper Ombudsmen www.newsombudsmen.org.

343 See for example the Minnesota News Council http://news-council.org.

Conclusion

4.29 United States privacy law consists of a complex set of constitutional, statutory and common-law protections, with significant variation from state to state. The constitutional traditions of the United States and New Zealand are so different that there is probably little that New Zealand can learn from US constitutional law relating to privacy, except in the area of Fourth Amendment jurisprudence on search and seizure. The main significance of United States constitutional law for New Zealand privacy law lies in the area of First Amendment jurisprudence, which is relevant to the need to balance privacy against the protection of freedom of expression in the New Zealand Bill of Rights Act 1990. New Zealand and the United States have also taken very different approaches to the regulation of use of personal information, with New Zealand opting for a comprehensive personal information protection law while the US has taken a sector-specific approach. The United States disclosure tort, and to a lesser extent the intrusion tort, have had a greater influence on New Zealand law than have other areas of US privacy law.

EUROPE

4.30 There are distinctive European approaches to privacy in both the general human rights field and the narrower field of personal data protection. Our focus here is on legal instruments relating to privacy that cover the Council of Europe and European Union (EU) states generally, rather than the privacy law of individual European jurisdictions. It is worth noting, however, that the civil law jurisdictions have generally given somewhat greater weight to privacy and somewhat less weight to freedom of expression than the common law jurisdictions.[344] This has undoubtedly influenced the approach to privacy by the pan-European institutions. However, there is evidence of convergence between common law and civil law jurisprudence under the influence of human rights instruments, with countries such as England giving greater protection to privacy and countries such as France giving greater recognition to freedom of expression than in the past.[345]

Human rights

4.31 Article 8 of the European Convention on Human Rights (ECHR) provides:

> *Article 8 – Right to respect for private and family life*
>
> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being

344 On French and German privacy law see Catherine Dupré "The Protection of Private Life Versus Freedom of Expression in French Law" and Rosalind English "Protection of Privacy and Freedom of Speech in Germany" in Madeleine Colvin (ed) *Developing Key Privacy Rights* (Hart Publishing, Oxford, 2002) 45, 77; James Q Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale LJ 1151; James Gordley "When is the Use of Foreign Law Possible? A Hard Case: The Protection of Privacy in Europe and the United States" (2007) 67 La L Rev 1073; New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 124-135.

345 Hilary Delany and Cliodhna Murphy "Towards Common Principles Relating to the Protection of Privacy Rights? An Analysis of Recent Developments in England and France and before the European Court of Human Rights" [2007] EHRLR 568.

of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4.32 It is balanced by article 10:

Article 10 – Freedom of expression

(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

4.33 Neither of these rights, which are enforceable against member states through the European Court of Human Rights, are absolute. Moreover, neither the text of the ECHR nor the jurisprudence of the European Court of Human Rights give one article precedence over the other. Where the two rights come into conflict, the Court will apply the principle of proportionality in order to assess the value of each in the particular circumstances. It has been argued, however, that despite the theoretical equality between the two articles, some recent decisions of the Court (particularly in the *von Hannover* case, discussed below) have placed "significant restrictions … on the enjoyment of Art.10 rights in order to protect a right to privacy".[346]

4.34 Under article 8, states have obligations not only to refrain from interfering with private life (negative obligations) but also positive obligations to provide protections for private life, including protections against interference by private actors. The Court has taken an expansive view of private life,[347] encompassing many matters that do not involve questions of privacy of the type that we are discussing in this Review. In addition to cases involving disclosure of personal information, surveillance, media intrusion and the like, the Court has found interferences in relation to questions of sexuality, family life and child-rearing, personal identity and rights to pursue a chosen lifestyle.[348] The Court has

346 Hilary Delany and Cliodhna Murphy "Towards Common Principles Relating to the Protection of Privacy Rights? An Analysis of Recent Developments in England and France and before the European Court of Human Rights" [2007] EHRLR 568, 570.

347 The Court has consistently stated that "Private life is a broad term not susceptible to exhaustive definition": see for example *Peck v United Kingdom* (2003) 33 EHRR 719 (Section IV, ECHR), para 57.

348 NA Moreham "The Right to Respect for Private Life in the European Convention on Human Rights: A Re-examination" [2008] EHRLR 44. Moreham identifies five categories of private life interest in the Court's article 8 jurisprudence.

increasingly employed the concept of "reasonable" or "legitimate" expectations of privacy in assessing claims under article 8, although it has not yet fully developed what it means by this concept.[349]

von Hannover v Germany

4.35 In *von Hannover v Germany,* the European Court of Human Rights considered the right to privacy as it applies to public space, public figures and the public interest. Princess Caroline of Monaco sought to prevent the popular press from publishing photographs of her in restaurants, on horseback, riding a bicycle, shopping, on a skiing holiday, leaving her residence, playing tennis, and engaging in other fairly innocuous activities. In a series of cases before the German courts, her applications had been successful in respect of some of the photos (including three photos showing her with her children) but not others.

4.36 Princess Caroline successfully applied to the European Court of Human Rights in relation to the remaining photographs, claiming that German law provided inadequate protection of her article 8 right to respect for her private life, and alleging that "she was constantly hounded by paparazzi who followed her every daily movement".[350] The Court found that "she should, in the circumstances of the case, have had a 'legitimate expectation' of protection of her private life", and that the German courts did not strike a fair balance between the competing interests.[351]

4.37 The Court considered that Princess Caroline was a private individual because she did not exercise any official functions on behalf of the Monacan state,[352] although it gave no reasons for adopting this approach to determining whether or not a person is a public figure. The Court also reiterated its previously-expressed view that there is a zone of a person's interaction with others, even in public, which may fall within the scope of "private life".[353]

4.38 In addition, the Court considered that the photographs and accompanying articles related exclusively to details of Princess Caroline's private life.[354] As Gavin Phillipson points out, the Court did not explain why the photos related to the Princess's private life, nor did it distinguish between the different photos.

---

349 The phrase "reasonable expectation of privacy" first appeared in ECHR jurisprudence in *Halford v United Kingdom* (1997) 24 EHRR 523 (ECHR), para 45. See H Tomás Gómez-Arostegui "Defining Private Life under the European Convention on Human Rights by Referring to Reasonable Expectations" (2005) 35 Cal W Int'l LJ 153, 165-175; Hilary Delany and Cliodhna Murphy "Towards Common Principles Relating to the Protection of Privacy Rights? An Analysis of Recent Developments in England and France and before the European Court of Human Rights" [2007] EHRLR 568, 580-581.

350 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 44.

351 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), paras 78-80. Two judges issued concurring opinions, but with somewhat different reasoning from that of the majority.

352 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), paras 62, 72.

353 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 50.

354 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), paras 64, 74, 76.

It seems that the Court used "private" to mean "non-official", in contrast to another common usage in which matters are private because of the nature of the facts or activities involved or of the spaces in which activities take place.[355]

4.39 The most significant part of the judgment of the European Court of Human Rights was its consideration of the balance between protection of private life and freedom of expression. The Court recognised that the freedom of expression guaranteed by article 10 of the ECHR "constitutes one of the essential foundations of a democratic society".[356] However, it drew a distinction between:[357]

> reporting facts – even controversial ones – capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions.

In the latter case, the Court said, the "watchdog" role of the press did not apply. The Court acknowledged that, in special circumstances, the public's right to be informed can extend to information about the private life of public figures (particularly politicians), but stated that the photos and articles in question were not "within the sphere of any political or public debate because … [they] relate exclusively to details of the applicant's private life."[358]

4.40 The Court made some other significant points which have a bearing on the balance between privacy and freedom of expression:

- While freedom of expression extends to the publication of photographs, the case was not concerned with "the dissemination of 'ideas', but of images containing very personal or even intimate 'information' about an individual".[359] There appears to be a suggestion here that images, not being "ideas", are less protected by article 10 than text.
- The context in which the photographs were taken is important. In particular, it is significant that the photos were taken without the subject's knowledge or consent, "and the harassment endured by many public figures in their daily lives cannot be fully disregarded".[360]
- The development of new communication technologies, which make it easier to store, reproduce and disseminate personal information, necessitates "increased vigilance in protecting private life".[361]

4.41 The Court concluded that "the decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the published photos and articles make to a debate of public interest". The Court considered "that the public does not have a legitimate interest in

355 Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) New Dimensions in Privacy Law: International and Comparative Perspectives (Cambridge University Press, Cambridge, 2006) 184, 203-204.

356 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 58.

357 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 63.

358 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 64.

359 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 59.

360 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 68 (see also para 59).

361 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), para 70.

knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public."[362]

4.42 The decision of the European Court of Human Rights in *von Hannover* raises particular difficulties for the developing English law of privacy, which we consider below.

Personal data protection

4.43 In *Privacy: Concepts and Issues* we discussed the 1981 Council of Europe Convention 108 and the 1995 European Union Directive 95/46/EC on data protection. The latter Directive has been implemented by member states through national legislation such as the United Kingdom's Data Protection Act 1998.[363] Also significant has been the work of the Article 29 Data Protection Working Party, established under Directive 95/46/EC as an independent advisory body, which has examined a wide range of informational privacy issues with a view to achieving greater consistency within the EU.

4.44 Another significant European data protection instrument is the 2002 EU Directive 2002/58/EC on privacy and electronic communications.[364] This widened the scope of the 1997 Directive that it replaced, "bring[ing] within the same regulatory framework all [publicly-accessible] services and networks whose main object is the transmission and routing of signals regardless of the technology used". This includes the internet, as well as data about communications traffic and locational data (information about the geographic position of a communications device such as a mobile phone).[365]

Conclusion

4.45 Although New Zealand is not a member of the European Union, European privacy law has some indirect influence on New Zealand. The ECHR is significant for New Zealand law in two ways. First, New Zealand courts have noted that the ECHR and the jurisprudence of the European Court of Human Rights "have persuasive weight" and "can be important in helping develop New Zealand

362 *von Hannover v Germany* (2005) 40 EHRR 1 (Section III, ECHR), paras 76-77.

363 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (28 January 1981) ETS 108; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281. Discussed in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 170-179.

364 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector [2002] OJ L201.

365 Yves Poullet with J Marc Dinant "The Internet and Private Life in Europe: Risks and Aspirations" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 60, 68.

jurisprudence".[366] Secondly, European jurisprudence may have an indirect influence on New Zealand common law through its influence on English law. As discussed below, the European influence on English common law is particularly significant in relation to privacy. European data protection law is also influential internationally, including in New Zealand, because of the provision in the European Union data protection Directive stating that personal information can only be transferred out of the EU to countries that ensure "an adequate level of protection" to that information. Given the important role of personal information in international commerce, this provision creates an economic incentive for countries to bring their informational privacy laws into line with the EU Directive.[367]

UNITED KINGDOM

4.46 The legal protection of privacy in the United Kingdom has been transformed over the past decade by the Human Rights Act 1998, which implements the United Kingdom's obligations under the ECHR. The Act has influenced the English courts in extending the action for breach of confidence to cover disclosure of private information. Privacy legislation has also been strongly influenced by the United Kingdom's membership of the European Union. Statutes such as the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000 are designed in large part to implement the United Kingdom's obligations under European data protection and human rights law. The United Kingdom has legislation dealing with personal information and some forms of intrusion and surveillance. There are also privacy codes governing the media.

Human Rights Act 1998

4.47 The Human Rights Act 1998, which largely came into force in October 2000, gives effect to specified rights under the ECHR, including the article 8 and article 10 rights to privacy and freedom of expression.[368] Public authorities are required to act in a manner compatible with these rights, and persons who claim that they have been the victims of breaches of Convention rights by public authorities may bring legal proceedings against these authorities.[369] Courts and tribunals are required to act in a way that is not incompatible with Convention rights.[370] Courts are also required to read and give effect to legislation in a way that is compatible with Convention rights,[371] and, in determining questions in connection with these rights, to take into account relevant judgments of the European Court of Human Rights.[372]

366 *Nicholls v Registrar of the Court of Appeal* [1998] 2 NZLR 385, 398 (CA) Eichelbaum CJ; *Hosking v Runting* [2005] 1 NZLR 1, para 53 (CA) Gault P and Blanchard J. The European Court of Human Rights was the most-cited international tribunal according a survey of reported New Zealand High Court, Court of Appeal and Supreme Court cases in which reference was made to overseas rights-based precedents from the enactment of the New Zealand Bill of Rights Act 1990 until April 2006: James Allan, Grant Huscroft and Nessa Lynch "The Citation of Overseas Authority in Rights Litigation in New Zealand: How Much Bark? How Much Bite?" (2007) 11 Otago LR 433, 438-439, 455.

367 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 176-178.

368 Human Rights Act 1998, s 1.

369 Human Rights Act 1998, ss 6-7.

370 Human Rights Act 1998, s 6(3)(a).

371 Human Rights Act 1998, s 3(1).

372 Human Rights Act 1998, s 2(1)(a).

4.48 Section 12(4) of the Act provides that, if a court is considering whether to grant any relief which might affect the exercise of the right to freedom of expression, it must have particular regard to the importance of that right. Furthermore, "where the proceedings relate to material which the respondent claims, or which appears to the court, to be journalistic, literary or artistic (or to conduct connected with such material)", the court is to have particular regard to the extent to which the material has, or is about to, become available to the public; the extent to which publication is, or would be, in the public interest; and "any relevant privacy code". Although this section might appear to give a privileged place to freedom of expression, the House of Lords has held that neither freedom of expression nor privacy takes precedence over the other, as we discuss further below.

4.49 It is clear that the Act does not create direct horizontal effect: a person cannot directly plead a breach of a Convention right by a private party before the courts. However, the courts have recognised some form of indirect horizontality, whereby a cause of action at common law will be interpreted in the light of Convention rights.[373]

Scots law

4.50 Scots law is a mixture of the civil and common law traditions, and is not constrained by the need to fit the protection of interests such as privacy into existing causes of action. Scots law has not yet recognised a specific right to privacy, but the influence of the Human Rights Act 1998 may lead the Scottish courts to take one of two available avenues for doing so. They could follow the English example of developing the law of breach of confidence,[374] or they could develop the actio iniuriarum, an action for the protection of honour and dignity received from Roman law. This second course, if pursued, could lead to a significant divergence between English and Scots law, and could allow Scots law to recognise intrusion into seclusion and interferences with bodily privacy as well as breaches of informational privacy.[375] While developments in Scots law may prove interesting, we confine our discussion of common law below to England and Wales, where privacy law is currently more developed and more influential on New Zealand.

English common law

4.51 We described in chapter 2 various causes of action in the common law of England and New Zealand which may protect privacy, including nuisance, trespass, intentional infliction of harm and passing off. A significant point of difference between English and New Zealand common law, however, is that the New Zealand Court of Appeal in *Hosking v Runting* recognised a tort of invasion

373 For more detailed discussion, with a particular focus on the implications for privacy, see Alison L Young "Horizontality and the Human Rights Act 1998" in Katja S Ziegler (ed) *Human Rights and Private Law: Privacy as Autonomy* (Hart Publishing, Oxford, 2007) 35.

374 In Scotland breach of confidence is part of the law of delict, equivalent to tort, rather than equity.

375 Hector L MacQueen "Searching for Privacy in a Mixed Jurisdiction" (2006) 21 Tul Eur & Civ LF 73; Elspeth Reid "*Wainwright v United Kingdom*: Bringing Human Rights Home?" (2007) 11 Edin LR 83, 87-88.

of privacy by public disclosure of private facts, while English law has dealt with the disclosure of private facts through the equitable action for breach of confidence.

4.52 English common law does not recognise a distinct tort of invasion of privacy, the suggestion that such a tort existed having been dismissed by the House of Lords in *Wainwright v Home Office*.[376] However, it is important to note that *Wainwright* concerned a strip search, so it involved bodily rather than informational privacy. In that case the Law Lords declined to find the existence of a "general" or "high-level" right to privacy. This does not, however, prevent the courts from employing more specific causes of action to protect particular aspects of privacy. A right to protection against misuse of private information has in effect been recognised by adapting breach of confidence. It is conceivable that the courts could in future also recognise a cause of action for invasion of privacy by covert recording or surveillance.[377]

Breach of confidence

4.53 Traditionally, breach of confidence protected information communicated by one person to another "in circumstances importing a duty of confidence";[378] that is, circumstances in which the person receiving the information knows that he or she should keep it secret. The requirement of a confidential relationship has now been dispensed with by the English courts.[379] This development began before the influence of the Human Rights Act 1998,[380] but has been given further impetus by the Act where the disclosure of private information is concerned. The Human Rights Act has also influenced the modification of the first part of the *Coco v Clark* test, which required that information must have the necessary quality of confidence about it. The courts will now recognise a breach of confidence where there is a disclosure of private facts, or facts in respect of which the plaintiff had a reasonable expectation of privacy.[381]

376 *Wainwright v Home Office* [2004] 2 AC 406, para 35 (HL) Lord Hoffman.

377 In *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), para 17, Eady J observed that "the very fact of clandestine recording may be regarded as an intrusion and an unacceptable infringement of Article 8 rights", but noted that the intrusive method of gathering information had not been pleaded in the case.

378 *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41, 47 Megarry J.

379 Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 184, 188-191; Tanya Aplin "The Future of Breach of Confidence and the Protection of Privacy" (2007) 7 OUCLJ 137, 141; Paul Stanley *The Law of Confidentiality: A Restatement* (Hart Publishing, Oxford, 2008) 4.

380 See, for example, *Attorney-General v Guardian Newspapers (No 2)* [1990] 1 AC 109, 281 (HL), where Lord Goff stated the duty of confidence in broad terms which could embrace situations such as "where an obviously confidential document is wafted by an electric fan out of a window into a crowded street, or where an obviously confidential document, such as a private diary, is dropped in a public place, and is then picked up by a passer-by."

381 Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 184, 192-202; Tanya Aplin "The Future of Breach of Confidence and the Protection of Privacy" (2007) 7 OUCLJ 137, 139; Paul Stanley *The Law of Confidentiality: A Restatement* (Hart Publishing, Oxford, 2008) 5-6.

4.54 The transformation of breach of confidence became clear in the decision of the House of Lords in *Campbell v MGN Ltd*.[382] This case concerned the revelation that a famous model was attending Narcotics Anonymous, the publication of details of her treatment, and the publication of photographs of her attending meetings. The House of Lords, by a majority of three to two, overturned the Court of Appeal's finding that there was no breach of confidence. All five Law Lords accepted that the action for breach of confidence could now provide a remedy for "misuse of private information" or "the unjustified publication of private information" (in the words of Lords Nicholls and Hoffmann, both in the minority).[383] The majority found liability in confidence despite the absence of a confidential relationship or of any indication of confidentiality (such as warning signs or security measures) at the place where the plaintiff was photographed. As Gavin Phillipson observes, "the only thing that could impose the obligation of confidence in relation to the photographs was the obviously private nature of the information itself – the fact that it concerned therapeutic treatment."[384]

4.55 While the House of Lords has expressed some discomfort at having been required to "shoehorn" the protection of private information within the cause of action for breach of confidence,[385] it is now clear that breach of confidence is the action by which the English courts will protect rights to informational privacy under article 8 of the ECHR. This does not mean, however, that what Buxton LJ has termed "old-fashioned breach of confidence"[386] has disappeared. In fact, a number of recent cases have involved both confidential relationships and the misuse of private information.[387]

Elements of the cause of action

4.56 The English courts have adopted a two-stage process, based on articles 8 and 10 of the ECHR, in determining claims for breach of confidence by disclosure of private facts. In *Ash v McKennitt*, Buxton LJ described the approach as follows:[388]

> the court has to decide two things. First, is the information private in the sense that it is in principle protected by article 8? If "no", that is the end of the case. If "yes", the second question arises: in all the circumstances, must the interest of the owner of the private information yield to the right of freedom of expression conferred on the publisher by article 10?

382 *Campbell v MGN Ltd* [2004] 2 AC 456 (HL).

383 *Campbell v MGN Ltd* [2004] 2 AC 456, paras 14, 51 (HL) Lord Nicholls, Lord Hoffmann.

384 Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 184, 190.

385 *Douglas and Others v Hello! Ltd and Others (No 3)* [2006] QB 125, para 53 (HL) Lord Phillips.

386 *McKennitt and Others v Ash and Another* [2008] QB 73, para 8 (CA) Buxton LJ.

387 Tanya Aplin "The Future of Breach of Confidence and the Protection of Privacy" (2007) 7 OUCLJ 137, 166-170. Examples of such cases are *McKennitt and Others v Ash and Another* [2008] QB 73 (CA); *Associated Newspapers Ltd v HRH Prince of Wales* [2008] Ch 105 (CA); *Lord Browne of Madingley v Associated Newspapers Ltd* [2008] QB 103 (CA).

388 *McKennitt and Others v Ash and Another* [2008] QB 73, para 11 (CA) Buxton LJ.

4.57 At the first stage, the courts will consider whether the facts disclosed are ones in respect of which the claimant had a reasonable expectation of privacy.[389] The test is an objective one: what the claimant was reasonably entitled to expect, rather than what he or she actually expected. A number of factors are relevant, including the subject matter, the form in which the information is conveyed and the way in which it was obtained. Where appropriate, the existence of a relationship of confidence between the parties will also be taken into account.[390]

4.58 The courts have accepted that there can be a reasonable expectation of privacy with respect to activities in a public place (as with the photographs in *Campbell*) and where information has already been circulated within a limited circle (as in the case of the Prince of Wales's diaries).[391] Furthermore, information may be private even if it is false.[392] In contrast to Gault P and Blanchard J's *Hosking* test, the English courts do not include a test of whether the publication would be highly offensive to a reasonable person. Where offensiveness of publication is taken into account, it appears that this will happen in the second stage, where privacy is balanced against freedom of expression.[393]

4.59 The second stage involves balancing the article 8 right to privacy against article 10, taking into account the particular facts of the case. Lord Steyn in *Re S (A Child)* distilled the principles to be followed in the balancing process:[394]

> First, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justifications for interfering with or restricting each right must be taken into account. Finally, the proportionality test must be applied to each.

This process involves a consideration of the type and subject matter of the speech or expression, and the strength of the privacy interests, involved. Other relevant factors include the extent to which the publication would add to information that is already publicly available, the accuracy or otherwise of the information, the degree to which the claimant is a public figure, whether the defendant is speaking about matters that are part of his or her own experience as well as the claimant's, and the nature and extent of the harm that would be caused by the disclosure.[395]

389 *Lord Browne of Madingley v Associated Newspapers Ltd* [2008] QB 103, para 24 (CA) Sir Anthony Clarke MR; *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), paras 7, 10 Eady J.

390 Paul Stanley *The Law of Confidentiality: A Restatement* (Hart Publishing, Oxford, 2008) 7-13.

391 With regard to the Prince of Wales's diaries see *Associated Newspapers Ltd v HRH Prince of Wales* [2008] Ch 105, paras 40-43 (CA) Phillips LCJ.

392 *McKennitt and Others v Ash and Another* [2008] QB 73, paras 80, 86 (CA) Buxton, Longmore LLJ; Paul Stanley *The Law of Confidentiality: A Restatement* (Hart Publishing, Oxford, 2008) 15-17.

393 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, paras 25-26, 39, 48-49 Sir Anthony Clarke MR. The Court of Appeal in *Murray* (para 25) quoted with approval the reasoning of Lord Nicholls in *Campbell* with regard to the "highly offensive" test: *Campbell v MGN Ltd* [2004] 2 AC 456, para 22 (HL).

394 *Re S (A Child) (Identification: Restrictions on Publication)* [2005] 1 AC 593, para 17 (HL) Lord Steyn.

395 Paul Stanley *The Law of Confidentiality: A Restatement* (Hart Publishing, Oxford, 2008) 91-96.

4.60 When it comes to weighing the value of freedom of expression, the court will evaluate the use to which the defendant has, or intends to, put this right.[396] An important consideration is the extent to which the publication contributes to a debate of legitimate public concern. Where it does not do so, it may well have to give way to the protection of privacy.[397] On this point, the English courts are in agreement with the decision of the European Court of Human Rights in *von Hannover*, but the courts in England and Strasbourg may differ on the interpretation of what is a matter of legitimate public interest.[398]

The English courts and von Hannover

4.61 Gavin Phillipson has commented that:[399]

> no sooner had the House of Lords [in *Campbell*] dragged the common law up to the standard of protection thought to be required by Article 8 than [the European Court of Human Rights in *von Hannover*] moved the goalposts – and quite some distance too.

In *von Hannover*, the European Court of Human Rights took an expansive view of the protection afforded to private life by article 8, and a restricted view of matters of legitimate public interest for the purpose of article 10. This approach is difficult to reconcile with the position that had been reached in England, and the implications for English law are still being worked through.

4.62 The implications of *von Hannover* were considered in *Murray*, which involved facts that are strikingly similar to those of *Hosking*. The son of Joanne Murray (who writes as JK Rowling) was photographed with his parents while he was being pushed in a buggy on an Edinburgh street, and the picture published. The Murrays brought a claim on their son's behalf for infringement of his right to privacy and misuse of private information in relation to the photograph. The photographic agency sought to strike out the claim, arguing that it had no real prospect of success.

4.63 In a strike-out action the High Court, Patten J noted that he started "with a strong predisposition to the view that routine acts such as the visit to the shop or the ride on the bus should not attract any reasonable expectation of

396 *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), para 15 Eady J. This approach contrasts with some earlier decisions, which did not assess the value of the speech claim in the particular circumstances of the case: Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 184, 213-219.

397 Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 184, 216.

398 Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 184, 219; Hilary Delany and Cliodhna Murphy "Towards Common Principles Relating to the Protection of Privacy Rights? An Analysis of Recent Developments in England and France and before the European Court of Human Rights" [2007] EHRLR 568, 574.

399 Gavin Phillipson "The 'Right' of Privacy in England and Strasbourg Compared" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 184, 185.

privacy."[400] He distinguished the case from *Campbell* on the grounds that the photographs in that case revealed private information concerning treatment for drug addiction, whereas the photograph of the claimant simply showed him being pushed along by his parents "on the most innocent and ordinary of occasions."[401] He also distinguished the case from *von Hannover* on the basis that there is a difference between showing a person engaged in family or leisure activities and showing "something as simple as a walk down a street or a visit to the grocers to buy the milk." Patten J held that this was a case in which there was no reasonable expectation of privacy with regard to innocuous activity in a public place and that, to the extent that *von Hannover* had expanded the scope of protection of private life beyond the position reached in *Campbell*, he was bound to follow *Campbell* in preference. He struck out the claim accordingly.[402]

4.64 On appeal, the Court of Appeal emphasised the fact that the claimant was a child.[403] It considered *Hosking v Runting*, on which Patten J had placed some reliance, and suggested that it was arguable that the English courts might take a different view from that of Gault P and Blanchard J as to reasonable expectations of privacy of children with regard to the publication of photographs without consent.[404] Sir Anthony Clarke MR stated that:[405]

> subject to the facts of the particular case, the law should indeed protect children from intrusive media attention, at any rate to the extent of holding that a child has a reasonable expectation that he or she will not be targeted in order to obtain photographs in a public place for publication which the person who took or procured the taking of the photographs knew would be objected to on behalf of the child. That is the context in which the photographs of David [Murray] were taken.

While the Court recognised that there may well be circumstances in which there will be no reasonable expectation of privacy, even after *von Hannover*, it will all depend on the facts of the particular case. It is not possible to draw a clear distinction between family and leisure activities and innocuous everyday activities, as Patten J had done.[406] In the circumstances it was not necessary to analyse *von Hannover* in detail, but the Court believed that its views were consistent with the decision in that case.[407] The Court directed that there be a trial of all the issues, unless the parties were able to reach a settlement.[408]

400 *Murray v Express Newspapers plc and Big Pictures (UK) Ltd* [2007] EWHC 1908 (Ch) para 66 Patten J.

401 *Murray v Express Newspapers plc and Big Pictures (UK) Ltd* [2007] EWHC 1908 (Ch) paras 26-27 Patten J.

402 *Murray v Express Newspapers plc and Big Pictures (UK) Ltd* [2007] EWHC 1908 (Ch) para 68 Patten J.

403 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, para 47 Sir Anthony Clarke MR.

404 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, paras 48-52 Sir Anthony Clarke MR.

405 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, para 57 Sir Anthony Clarke MR.

406 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, para 55 Sir Anthony Clarke MR.

407 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, paras 59-60 Sir Anthony Clarke MR.

408 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, paras 61, 64 Sir Anthony Clarke MR.

4.65 At the time of writing, *Murray* has progressed no further.[409] It is also important to note that neither court in this case has so far been required to conduct the balancing exercise between articles 8 and 10. Important issues about the scope of article 8 and the balance between articles 8 and 10 remain to be considered by the English courts in the wake of *von Hannover*.

Conclusion

4.66 The English courts now recognise a cause of action for the public disclosure of private facts. Unlike in New Zealand, however, where a separate disclosure tort has been recognised, the English courts have extended the action for breach of confidence. Two other major distinctions can be drawn between the causes of action in England and New Zealand, based on the case law so far.

4.67 First, the English courts do not require claimants to show that the publicity given to private facts would be highly offensive to an objective, reasonable person in order to establish that there has been a breach of their privacy. The New Zealand courts do employ the "highly offensive" criterion as a threshold test.

4.68 Secondly, the English courts have stated clearly that neither privacy nor freedom of expression takes precedence over the other. Both are recognised in the ECHR, which was given domestic effect by the Human Rights Act 1998. An express right to privacy was deliberately left out of the New Zealand Bill of Rights Act 1990, whereas the right to freedom of expression is recognised in the Act. While the New Zealand courts have recognised that protection of privacy can act as a justifiable limit on freedom of expression in some circumstances, it is not yet clear whether the courts will treat privacy and freedom of expression as rights of equal value.

4.69 Another significant distinction concerns the claimants in the English privacy cases. The English cases have had a major focus on intrusion by the media into the lives of celebrities or other prominent public figures. By contrast, only a few New Zealand privacy cases so far have involved celebrities. This difference arguably reflects the more highly-developed celebrity culture, and the more aggressive nature of the media, in Britain.

Legislation

4.70 The United Kingdom's statutory framework for the protection of privacy is in many respects similar to New Zealand's. The main statute protecting personal information is the Data Protection Act 1998, which came into force in March 2000. This Act (which replaced the Data Protection Act 1984) implements the United Kingdom's responsibilities under the European Union Directive 95/46/EC. The Act is the responsibility of the Information Commissioner, who also administers the Freedom of Information Act 2000. The Data Protection Act 1998 is a principles-based statute which applies to organisations in both the public and private sectors.

409 Permission to appeal the Court of Appeal's decision to the House of Lords was declined: "Big Pictures Appeal Against Harry Potter Author JK Rowling Privacy Ruling is Rejected" (28 October 2008) www.pressgazette.co.uk (accessed 29 October 2008).

4.71 While the Data Protection Act 1998 is similar in a number of respects to New Zealand's Privacy Act 1993, there are also some significant differences. Features of the Data Protection Act 1998 not found in the Privacy Act 1993 (NZ) include:

- Persons processing personal data (known as "data controllers") must be registered with the Information Commissioner. It is an offence to process data without registration (ss 17, 21(1)).
- While complaints may be taken to the Information Commissioner, certain rights of data subjects under the Act may also be enforced directly in the courts (ss 7-14). The courts may award compensation for damage suffered as a result of breaches of the Act, and may also order data controllers to take steps to comply with the requirements of the Act or to rectify breaches.
- The Act includes a number of criminal offences.[410] Perhaps the most significant of these concerns knowingly or recklessly obtaining, disclosing, or procuring the disclosure of personal information without the consent of the data controller, or selling personal data obtained in this way (s 55). This offence is currently punishable by a fine.[411]
- As discussed further below, there is an exemption in the Act for journalism, but this does not comprehensively exclude the news media from the operation of the Act.

4.72 Other statutes provide protection against intrusion. The Protection from Harassment Act 1997 makes harassment an offence and also allows civil claims to be brought for harassment. In contrast to New Zeland's Harassment Act 1997, the UK Act provides for the award of damages for harassment.[412] In a recent case, the actress Sienna Miller won £53,000 damages in a case brought under the Act for harassment by paparazzi.[413] Section 67 of the Sexual Offences Act 2003 makes it an offence to observe or record another person doing a private act, where the observer or recorder does so for the purpose of sexual gratification and where the other person does not consent.[414]

4.73 The main statute dealing with surveillance is the Regulation of Investigatory Powers Act 2000 (RIPA). This Act was passed to bring the use of surveillance by public authorities into line with the Human Rights Act 1998, and particularly with article 8 of the ECHR. Hopes that RIPA would provide a single, comprehensive legal framework for surveillance, perhaps extending to

410 There are some offences in the Privacy Act 1993 (NZ), s 127, but these relate to matters such as obstructing, failing to comply with or misleading the Commissioner, rather than misuse of personal information.

411 The Criminal Justice and Immigration Act 2008, s 77, provides that the Secretary of State may by order provide for a person who is guilty of an offence under section 55 of the Data Protection Act to be liable to imprisonment. This section is not yet in force. Section 144 of the Criminal Justice and Immigration Act 2008, also not yet in force, provides for civil penalties for serious breaches of data protection principles by data controllers.

412 Protection from Harassment Act 1997, ss 3(2), 8(5)(a), 8(6). Section 3 applies to England and Wales and section 8 to Scotland.

413 David Brown "Sienna Miller Wins £50,000 Payout from Paparazzi" (22 November 2008) *The Times* www.timesonline.co.uk (accessed 24 November 2008).

414 Section 68 states that a person is doing a private act if the person is in a place which would reasonably be expected to provide privacy, and the person's genitals, buttocks or breasts are exposed or covered only with underwear; the person is using the lavatory; or the person is doing a sexual act of a kind not ordinarily done in public.

surveillance by "unscrupulous private persons", were not realised.[415] The Act does, however, provide some protections against intrusions into privacy by surveillance. Part I of RIPA deals with interception of communications. Section 1 makes it an offence intentionally and without lawful authority to intercept a communication in the course of its transmission by a public postal service or a telecommunications system. Part I also provides blanket permissions for the interception of communications in certain circumstances, and provides for interception warrants.

4.74 Part II of RIPA deals with surveillance in general carried out by public authorities. It does not criminalise surveillance carried out by unauthorised persons, but instead makes authorised surveillance lawful (s 27). Unauthorised surveillance by a public authority would in many cases be in breach of the Human Rights Act 1998. There are no general restrictions on surveillance by private persons, however. The provisions relating to authorisation of surveillance are not directly relevant this issues paper, but there are two points worth noting:

- Surveillance is defined broadly in the Act (section 48(2)). It includes, but is not restricted to, the use of surveillance devices.
- Since the Act was passed, the range of public authorities that may undertake some forms of authorised surveillance has increased. It now includes local authorities and a number of regulatory bodies that would not normally be considered law enforcement agencies.[416]

Regulation of the media

4.75 The Office of Communications (Ofcom) is responsible for the regulation of broadcasting, telecommunications and wireless communications.[417] Among other things, it is required to apply standards that provide adequate protection to the public against "unwarranted infringements of privacy" by television and radio broadcasters.[418] Section 8 of the Ofcom Broadcasting Code deals with privacy in some detail, and addresses intrusive methods of gathering material as well as the nature of the material that is broadcast. Individuals may complain to Ofcom about breaches of the privacy standards. If Ofcom finds that there has been a breach, it may impose a range of sanctions against broadcasters, including fines and directions requiring that its decisions be broadcast or prohibiting the further broadcast of offending material.[419]

4.76 Newspapers and magazines are covered by the Press Complaints Commission, a self-regulatory body established by the print media industry.[420] Its code of practice includes a number of general and specific clauses relating to aspects

415 Yaman Akdeniz, Nick Taylor and Clive Walker "Regulation of Investigatory Powers Act 2000 (1): BigBrother.gov.uk: State Surveillance in the Age of Information and Rights" [2001] Crim LR 73, 90.

416 Christopher Hope "Local Authorities Launched 10,000 Snooping Operations Last Year" (23 July 2008) *Telegraph* www.telegraph.co.uk (accessed 23 July 2008).

417 See www.ofcom.org.uk.

418 Communications Act 2003 (UK), s 3(2)(f)(ii).

419 Mark Thomson "Privacy and the Media" (April 2005) www.carter-ruck.com (accessed 14 August 2008); Liberty *Overlooked: Surveillance and Personal Privacy in Modern Britain* (2007) 79.

420 See www.pcc.org.uk and House of Commons Culture, Media and Sport Committee "Self-Regulation of the Press" (HC 375, 2007).

of privacy.[421] Like the Ofcom code, it covers intrusive methods of gathering information as well as publication of private information. Clause 10 provides, in part:

> The press must not seek to obtain or publish material acquired by using hidden cameras or clandestine listening devices; or by intercepting private or mobile telephone calls, messages or emails; or by the unauthorised removal of documents or photographs; or by accessing digitally-held private information without consent.

However, this clause, like a number of other clauses relating to privacy, is qualified by an exception where the material can be demonstrated to be in the public interest, and the code notes that "There is a public interest in freedom of expression itself." Complaints about breaches of the code are considered by the Commission and, where it appears that there may have been a breach, the Commission will try to resolve the breach to the complainant's satisfaction. If the complaint cannot be resolved and is upheld, the Commission can require the publication to publish with due prominence the decision upholding the complaint.

4.77 In contrast to New Zealand's Privacy Act, the news media are not entirely excluded from the coverage of the Data Protection Act 1998. Section 32 of the Act provides an exemption from most of the Act's principles and several of the rights of data subjects for the publication of "journalistic, literary or artistic material". However, the data controller must reasonably believe, having regard to the public interest in freedom of expression, that the publication would be in the public interest, and that compliance with the Act would be incompatible with journalistic, literary or artistic purposes. The Act does not define "public interest", but does say that, in determining whether publication is in the public interest, regard may be had to compliance with any relevant code of practice designated by the Secretary of State for the purposes of section 32. The Broadcasting and Press Complaints Commission codes have been so designated.[422] In cases in which journalistic publication is deemed not to be exempt under section 32, compensation can be awarded for distress caused by a breach of the Act.[423] In a number of major privacy cases (including *Campbell, Douglas* and *Murray*), breach of the Data Protection Act has been pleaded in addition to breach of confidence.

Conclusion

4.78 The most significant difference between the legal protection of privacy in the United Kingdom and in New Zealand is that, by enacting the Human Rights Act 1998, the United Kingdom has recognised a right to privacy that has equal status with the right to freedom of expression and other rights. This has created a general right to protection against interference with privacy by the state in the United Kingdom, and has led the English courts to recognise a right to protection

421 Clauses 3-11 all have some relevance to privacy. See www.editorscode.org.uk for more detail on the PCC code.

422 "Data Protection Act, Journalism and the PCC Code" (Guidance Note Issued by the Press Complaints Commission in co-operation with the Information Commissioner, 2005) www.editorscode.org.uk (accessed 25 August 2008).

423 Data Protection Act 1998, s 13(2)(b).

against disclosure of private information that applies between private parties. There is no express protection of privacy in the New Zealand Bill of Rights Act 1990. However, the New Zealand courts have recognised a civil action for disclosure of private facts, albeit by a different legal route than the English courts. There are many similarities in the legislative framework for protecting privacy in the two countries, although the Data Protection Act 1998 (UK) differs in some significant respects from its New Zealand equivalent. Regulation of the media is also similar in both countries, but the United Kingdom codes covering broadcasting and the print media are much more detailed with respect to privacy than the codes of the Broadcasting Standards Authority and the Press Council in New Zealand.

REPUBLIC OF IRELAND

4.79 The Irish courts have developed an action for breach of privacy. The Irish Constitution, like the United States Constitution, does not contain an express guarantee of privacy, but the courts have nonetheless held that it is an "unenumerated" or implied right. In *Kennedy v Ireland* in 1987, a case involving the unlawful tapping of the plaintiff's telephone line, Hamilton J said: "Though not specifically guaranteed by the constitution the right of privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the state."[424]

4.80 There has been a small number of cases but they are significant. In *Herrity v Associated Newspapers (Ireland) Limited*, Dunne J summarised the principles emerging from the cases as follows:[425]

(i) There is a Constitutional right to privacy.

(ii) The right to privacy is not an unqualified right.

(iii) The right to privacy may have to be balanced against other competing rights or interests.

(iv) The right to privacy may be derived from the nature of the information at issue – that is, matters which are entirely private to an individual and which it may be validly contended that there is no proper basis for the disclosure either to third parties or to the public generally.

(v) There may be circumstances in which an individual may not be able to maintain that the information concerned must always be kept private, having regard to the competing interests which may be involved, but may make complaint in relation to the manner in which the information was obtained.

(vi) The right to sue for damages for the breach of the constitutional right to privacy is not confined to actions against the State or State bodies or institutions.

4.81 In the *Herrity* case itself, the plaintiff sued following the publication of material about her marriage and her relationship with a Catholic priest. A newspaper published, among other things, extracts from recordings of a private conversation with the priest which had been obtained by unlawful telephone tapping. Dunne J gave judgment for the plaintiff. Noting that privacy cases such as this involve a balancing of interests, he concluded that as a general proposition cases in which the right to privacy will prevail over the right to freedom of expression may well be few and far between. However, in this case the unlawful obtaining of the information made a difference, and the plaintiff's privacy rights overrode

424 *Kennedy v Ireland* [1987] 1 IR 587, 592.

425 *Herrity v Associated Newspapers (Ireland) Limited* [2008] IEHC 249.

freedom of expression and indeed any other public interest considerations. He awarded damages of €60,000 for the conscious and deliberate breach and the distress which it caused, and a further €30,000 in punitive damages.

4.82 Two matters deserve comment. First, the quantum of damages is significant. It does not stand alone. Indeed, in a number of cases the Irish courts have awarded damages at a level far higher than those awarded in England. In addition to *Herrity* there have been awards of IR£100,000[426] and €70,000.[427]

4.83 Secondly, a number of the Irish cases draw a distinction between the publication of information which is inherently private and which there will seldom be reason for publishing and information of a kind not so intensely private but where the major cause of complaint is the method by which the information was obtained. In the *Herrity* case both dimensions were present. In *Cogley v Radio Telifís Éireann*,[428] a secret camera had been used to film activities in a nursing home. Noting that the method of obtaining the information was the major breach of privacy, the court nevertheless found it was outweighed by public interest and thus that an injunction would not issue.

4.84 The Irish cases are an interesting illustration of bold judicial activity which, as in New Zealand, has resulted in a new tort. The difference from the New Zealand position, of course, is that in Ireland there was held to be a constitutional basis for the development.

4.85 In December 2003, the European Convention on Human Rights Act 2003 came into force in Ireland. The Act imposes an obligation on the state to conduct itself in a manner which does not breach the rights of persons guaranteed by the Convention. Section 3 provides, in part:

> (1) Subject to any statutory provision (other than this Act) or rule of law, every organ of the State shall perform its functions in a manner compatible with the State's obligations under the Convention provisions.
>
> (2) A person who has suffered injury, loss or damage as a result of a contravention of sub-section (1), may, if no other remedy in damages is available, institute proceedings to recover damages in respect of the contravention in the High Court (or, subject to sub-section (3), in the Circuit Court) and the Court may award the person such damages (if any) as it considers appropriate.

It is not clear whether this legislation will make any difference to the protection of privacy in the Irish courts. The facts of *Herrity* occurred before it came into force, and Dunne J found it unnecessary to make any pronouncements about it.

426 *Hanahoe v Judge Hussey* [1998] 3 IR 69.

427 *Gray v MJELR* [2007] IEHC 52.

428 [2005] 2 ILRM 529.

4.86 In March 2006 a Working Group on Privacy, appointed by the Government, issued a Report[429] in which it recommended the statutory enactment of a dedicated tort of privacy. The Report noted that the courts had decided that privacy was a constitutional right: [430]

> If the citizens of the State enjoy (as they do) a constitutional right to privacy, they are entitled to expect that the legislature will provide them with a clear mechanism for enforcing that right; it is not satisfactory that they should have to await the happenstance of case law or judicial determination before they can do so.

The Government approved publication of the draft Privacy Bill based on the Working Group's recommendations, but in 2007 announced that it had decided to postpone progress on it.[431]

AUSTRALIA

4.87 The current landscape in Australia includes Federal and state information privacy legislation, some sector-specific privacy legislation at state level, regulation of the media and some criminal sanctions. Regarding civil causes of action for invasion of privacy, however, the current position in Australia is unclear. There have been some indications by the courts that a tort of invasion of privacy may exist in Australia. The Australian Law Reform Commission has recommended the enactment of a statutory cause of action for invasion of privacy.

Constitutional protection of privacy

4.88 Privacy is not protected in the Australian Constitution. Two states have human rights documents that include privacy. Part 2 of the Victorian Charter of Human Rights and Responsibilities Act 2006 includes the right of a person not to be subject to unlawful or arbitrary interference with his or her privacy, family, home or correspondence. The Act requires statutory provisions to be interpreted in a way that is compatible with the human rights set out under Part 2 and requires public authorities to act in a way that is compatible with those human rights. Section 12 of the Australian Capital Territory Human Rights Act 2004 provides that all individuals have the right not to have unlawful or arbitrary interferences with their privacy, family, home or correspondence or have their reputation unlawfully attacked. The Act also imposes a duty of consistent interpretation in respect of other legislation. Under the Act, when a court is interpreting an ACT law it must adopt an interpretation "consistent with human rights" as far as possible.

Privacy torts

4.89 The question of whether there might be a tort of invasion of privacy has been considered in Australia for some time. Historically, the development of privacy law has been regarded as restricted by the decision of the High Court of Australia

429 Working Group on Privacy *Report of Working Group on Privacy* (31 March 2006). See also the earlier report by the Law Reform Commission of Ireland *Privacy: Surveillance and the Interception of Communications* (LRC 57-1998, Dublin, 1998).

430 Working Group on Privacy *Report of Working Group on Privacy* (31 March 2006) para 6.05.

431 "New Libel Law is Top Priority as Privacy Bill is shelved" (12 November 2007) *The Independent* Dublin 26.

in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*.[432] There, Chief Justice Latham stated that "no authority was cited which shows that any general right of privacy exists." This was regarded for the next 60 years as authority that Australian law does not recognise a general right to privacy.

4.90 However, in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*,[433] the High Court indicated that the decision in *Victoria Park* does not preclude the recognition of a cause of action for invasion of privacy. Callinan J commented that:[434]

> it seems to me that … the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made.

Similarly, Gleeson CJ argued that "the law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy."[435] However, he thought that the courts ought to be cautious in declaring the existence of a tort, due to the lack of precision around the concept of privacy and the tension between privacy and free speech interests. He also felt that a tort may not apply to corporations, given that privacy protects human dignity.[436]

4.91 Gummow and Hayne JJ (with whom Gaudron J agreed) concluded that legal protection of privacy was based on the fundamental value of personal autonomy, which can only be invoked by natural persons, not corporations. Thus, a remedy based on privacy was not available to the plaintiffs in this case, being a corporation.[437] Kirby J preferred to postpone addressing the issue of privacy, as equity and statute law could be used to give the plaintiffs a remedy in this case.[438]

4.92 It is important to note that the Court's comments on the tort were not necessary to the decision. The Court appeared to leave the door open to a number of possibilities. Therefore, the decision should not be taken as declaring a tort of invasion of privacy.[439]

4.93 Following *Lenah* were two cases in which lower courts were prepared to find that a cause of action for invasion of privacy is part of the law of Australia. In the first case, *Grosse v Purvis*,[440] the Queensland District Court held that a tort of invasion of privacy does exist. It also enumerated the essential elements of the cause of action, as being a willed act by the defendant which intrudes upon the privacy or seclusion of the plaintiff in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities, and which

---

432 (1937) 58 CLR 479.

433 (2001) 208 CLR 199.

434 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, para 335.

435 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, para 40.

436 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, paras 41 and 43.

437 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, para 132.

438 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, para 188.

439 John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, Melbourne, 2005) 244.

440 (2003) Aust Torts Rep 81.

causes the plaintiff detriment in the form of mental, physiological or emotional harm or distress, or which prevents or hinders the plaintiff from doing an act which he or she is lawfully entitled to do. The court was also of the view that a defence of public interest should be available.

4.94 In a second case, *Jane Doe v Australian Broadcasting Corporation*,[441] the County Court of Victoria held that the defendant had invaded the plaintiff's privacy by unjustifiably publishing personal information about her, in circumstances where the plaintiff had a reasonable expectation of privacy. This amounted to an actionable wrong. In coming to this conclusion, the court relied on *Lenah Game Meats* and English cases, which it viewed as demonstrating a growing trend towards recognition of privacy as a right in itself deserving of protection.

4.95 Despite these cases indicating that a cause of action for invasion of privacy may be developing in Australia, a number of recent cases have found that no such cause of action exists. Importantly, these cases have been in superior courts.

4.96 First, in *Giller v Procopets*,[442] the Supreme Court of Victoria rejected a claim for invasion of privacy. The court felt that "the law has not developed to the point where the law in Australia recognises an action for breach of privacy." On appeal, the Court of Appeal found that a claim was available to the plaintiff in breach of confidence, and it was therefore unnecessary to decide whether a tort of invasion of privacy should be recognised.[443]

4.97 In a second case, *Milne v Haynes*,[444] the Supreme Court of New South Wales similarly held that there is as yet no recognition of a tort of breach of privacy in New South Wales.

4.98 In *Moore-Mcquillan v Work Cover Corporation*,[445] the Supreme Court of South Australia accepted that the current law was as stated in *Lenah.*

4.99 None of these three cases considered the decision in *Grosse v Purvis*. However, a case in the Federal Court, *Kalaba v Commonwealth of Australia*,[446] did so. The Federal Court expressly refused to adopt *Grosse* and concluded that the weight of authority indicates that a cause of action for invasion of privacy does not currently exist. In the most recent High Court of Australia reference to privacy, Callinan J reiterated his view in *Lenah* that the time was ripe for at least consideration of recognition of a cause of action for invasion of privacy.[447]

Law reform proposals

4.100 Both the Australian and New South Wales Law Reform Commissions have been engaged in reviews of privacy law. In 2007, the New South Wales Law Reform Commission (NSWLRC) released a consultation paper on a proposed statutory

441 [2007] VCC 281.

442 [2004] VSC 113.

443 [2008] VSCA 236.

444 [2005] NSWSC 1107.

445 [2007] SASC 55.

446 [2004] FCA 763.

447 *Batistatos v Roads and Traffic Authority of New South Wales* [2006] HCA 27.

cause of action for invasion of privacy.[448] The Commission proposes that, if a statutory cause of action were to be introduced, the statute should identify its objects and purposes and contain a non-exhaustive list of the types of invasion that fall within it. In its paper, it raises many of the same issues that we consider in chapters 6 and 7 below.

4.101 The Australian Law Reform Commission (ALRC) released its final report on privacy in August 2008.[449] The Commission recommends that Federal legislation should provide for a statutory cause of action for a serious invasion of privacy. In making this recommendation the Commission acknowledged that media organisations had expressed concern about the development of the cause of action. However, it noted that there was strong support for the development of a cause of action in the rest of the community, including among human rights and public interest organisations.[450]

4.102 The ALRC's proposed cause of action would contain a non-exhaustive list of types of invasion of privacy covered by the cause of action, such as where:[451]

- there has been an interference with an individual's home or family life;
- an individual has been subjected to unauthorised surveillance;
- an individual's correspondence or private communication has been interfered with; or
- sensitive facts about an individual's private life have been disclosed.

It would apply only where the individual had a reasonable expectation of privacy, and the act or conduct complained of was highly offensive to a reasonable person of ordinary sensibilities. The court would be required to consider whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest in informing the public about matters of public concern and the interest in allowing freedom of expression).[452] Courts would be empowered to offer a range of tailored remedies, including the award of aggravated (but not exemplary) damages, as well as injunctions, declarations and orders for apologies and corrections.[453]

4.103 Some of the reasons identified by the ALRC for favouring a statutory cause of action were that it does not involve the inconsistencies apparent in the development of the common law, allows for a more flexible approach to defences and remedies, and better guarantees that privacy will be protected in a broad range of contexts.[454] The key reasons identified by the NSWLRC were that there

448 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007).

449 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008).

450 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 2557-2560.

451 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) R74-1.

452 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) R74-2.

453 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) R74-5.

454 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 2564-7.

is currently no broad protection of privacy in Australian civil law, that the current social environment is perceived as being "increasingly invasive" of privacy, and that it would give effect to Australia's international obligations and accord with trends in other countries.[455] While the NSWLRC recognised benefits in leaving the development of a cause of action to the courts, it thought that a cause of action would be unlikely to develop if left to the common law.[456]

4.104 These proposals have not been well received by the Australian media. Generally, they have been criticised as an assault on the media and freedom of expression. The Federal Government seems to have taken the negative media response to the ALRC's proposed cause of action on board, and does not intend to progress the proposal at this point in time.[457]

4.105 Two state Law Reform Commissions have also specifically considered surveillance.[458] The NSWLRC proposed a new Surveillance Act, and we discuss their proposals in more detail in Part 3.

Privacy legislation

4.106 Australia's main Federal privacy law is the Privacy Act 1988 (Cth). Its content is similar to New Zealand's Privacy Act 1993. It is also principles-based, with broadly similar Privacy Principles. Like in New Zealand, there is a Privacy Commissioner with the power to investigate complaints about breaches of the Act. However, unlike in New Zealand, the Australian Commissioner has the power to make a determination in relation to complaints.[459]

4.107 The Act applies to Federal and Australian Capital Territory government agencies. However, it does not uniformly cover the private sector. Originally it only applied to the Federal public sector, but it was expanded in 2000 to cover some parts of the private sector, including all health service providers. Small businesses are currently exempt from the Act.[460] There are two sets of Privacy Principles: the Information Privacy Principles, which apply to the public sector, and National Privacy Principles for the private sector.

4.108 At state level, New South Wales, the Northern Territory and Victoria have legislation regulating the public sector that is similar to the Federal Privacy Act. However, other states do not have any information privacy legislation. Some states have also passed privacy legislation governing particular sectors.

---

455 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 12-15.

456 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 17.

457 Chris Merritt and Nicola Berkovic "Business to Carry Red-Tape Cost of Privacy Reform" (12 August 2008) *The Australian* www.theaustralian.news.com.au (accessed 12 August 2008).

458 New South Wales Law Reform Commission *Surveillance: Interim Report* (NSWLRC R98, Sydney, 2001) and *Surveillance: Final Report* (NSWLRC R108, Sydney, 2005). The Victorian Law Reform Commission is also currently working on a project on surveillance in public places: www.lawreform.vic.gov.au.

459 Privacy Act 1988 (Cth), s 52.

460 But see Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) R39-1.

For example, New South Wales has the Health Records and Information Privacy Act 2002 and the Workplace Surveillance Act 2005. Similarly, Victoria has the Health Records Act 2001.[461]

Regulation of the media

4.109 The Australian Communications and Media Authority (ACMA) is the statutory body that regulates the media, including broadcasting, online content[462] and telecommunications.[463] The ACMA encourages the development of industry codes of practice, and registers codes once they are developed. There are a number of codes covering different industry sectors, such as commercial television, subscription television, commercial radio and the internet. Many codes contain a privacy standard.[464]

4.110 Complaints about breaches of industry codes by broadcasters must first be made to the broadcaster concerned, and complainants who are not satisfied with a broadcaster's response can complain to the ACMA. If it finds a breach of a code, the ACMA may accept an enforceable undertaking by the broadcaster to ensure future compliance with the code, or may impose an additional licence condition requiring broadcasters to comply with the code. If a broadcaster breaches such an additional licence condition, the ACMA may issue a remedial direction requiring compliance. If the broadcaster fails to comply with the remedial direction, the ACMA has a number of options, including pursuing a civil penalty, referring the matter for prosecution as an offence, and suspending or cancelling the licence.[465]

4.111 Australia has a Press Council similar to New Zealand's. Its Statement of Principles includes a Privacy principle, which states that:[466]

> [r]eaders of publications are entitled to have news and comment presented to them honestly and fairly, and with respect for the privacy and sensibilities of individuals. However, the right to privacy should not prevent publication of matters of public record or obvious or significant public interest.

It also has more detailed Privacy Standards, which cover matters including collection, use, disclosure, quality and security of personal information.

461 Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (The Federation Press, Sydney, 2005) 99-100.

462 The ACMA's responsibilities in relation to online content include investigating complaints, encouraging the development of codes of practice and monitoring existing codes, providing advice and information about online safety, enforcing the Spam Act 2003 (Cth), and assisting in protecting against computer fraud and identity theft.

463 See Australian Communications and Media Authority Act 2005 (Cth) and Australian Communications and Media Authority "About Communications & Media Regulation" www.acma.gov.au (accessed 10 June 2008).

464 See Australian Communications and Media Authority *Privacy Guidelines for Broadcasters* (Sydney, 2005), which includes relevant extracts from broadcasting codes of practice.

465 The ACMA's complaints process and powers are summarised in Australian Communications and Media Authority "ACMA Finds that TCN 9 Breached Privacy Provisions of the Code" (27 November 2008) Press Release, www.acma.gov.au (accessed 4 December 2008).

466 Australian Press Council "Objects, Principles and Complaints Procedure" www.presscouncil.org.au (accessed 10 June 2008).

Criminal sanctions

4.112 Like New Zealand, Australia has some criminal offences related to invasion of privacy, which appear to have developed over time in response to particular issues and needs, rather than being driven by any underlying privacy framework. Offences exist particularly in the area of telecommunications and electronic surveillance. The Telecommunications (Interception) Act 1979 (Cth) prohibits the interception of communications over the telephone system. Regulation of telecommunications falls under the Federal jurisdiction, therefore there are no state laws on this subject.[467] Most states prevent the use of electronic devices to listen to conversations or observe activities that take place on private property. Under these state laws it is generally an offence for a person to install, use or maintain listening or surveillance devices to monitor or record private conversations or activities to which they are not a party. Laws also generally restrict publication or communication of records or reports of conversations or activities obtained through the use of a listening or surveillance device.[468]

Conclusion

4.113 Australian law currently protects privacy through Federal and state information privacy legislation, state legislation covering specific areas of privacy, regulation of the media and some criminal sanctions. As yet there is no settled cause of action for invasion of privacy. The higher courts have not recognised a privacy tort and, in the face of strong media opposition, it is yet to be seen whether law reform recommendations for a statutory cause of action for invasion of privacy will be adopted by the Federal or state governments.

CANADA

4.114 The Canadian landscape includes tort protection, information privacy legislation, some constitutional protection, criminal offences and regulation of the media. A particular feature of Canadian law is the existence of a statutory tort of invasion of privacy in several provinces. The regulatory framework, however, is somewhat patchy. It is important to note that protection of privacy takes place at both provincial and Federal levels in Canada. This section considers both, but with a focus on the Federal level.

Constitutional protection of privacy

4.115 Canada's Charter of Rights and Freedoms ("the Charter") does not specifically provide a right to privacy. However, the Charter has played an important role in the recognition of privacy as a value deserving legal protection.[469]

4.116 Several provisions of the Charter have been interpreted as encompassing protection of privacy. The most important is section 8 of the Charter, which provides that everyone has the right to be secure against unreasonable search and seizure. The Supreme Court has held that this right embodies the

467 Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (The Federation Press, Sydney, 2005) 99 and 141.

468 Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (The Federation Press, Sydney, 2005) 142 and 146-147.

469 Colin H H McNairn and Alexander K Scott *Privacy Law in Canada* (Butterworths, Markham (ON), 2001) 17.

right to be let alone by other people.[470] In practice, this means that privacy is used as a measure of whether a search or seizure is unreasonable. The issue is whether the privacy interest of the individual is outweighed by the public interest in which the government is acting. While the right to privacy is only secure against government interference when the interference occurs through a search or seizure, the courts have interpreted the concepts of search and seizure quite widely.[471] The Supreme Court has also held that the Charter protects privacy under the ambit of section 7, which provides that everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.[472]

4.117 In addition, the province of Québec expressly guarantees the right to respect for private life in section 5 of its Charter of Human Rights and Freedoms. In *Aubry v Éditions Vice-Versa*, the Supreme Court of Canada held that publication in a magazine of a photograph taken without the plaintiff's consent was a breach of section 5.[473]

Statutory torts

4.118 Four Canadian provinces have enacted similar statutes providing a cause of action for violation of privacy.[474] A statutory cause of action was also proposed in Ontario, but failed to gain Cabinet approval.[475] There have been few cases brought under the various statutes, and in general success rates have been low.

4.119 The province of Québec, which has a civil law system based on that of France, also protects the right to privacy in its Civil Code. The Code provides examples of actions that may be considered invasions of privacy.[476] Our discussion of the statutory torts is restricted to the torts of the common-law provinces.

470 *Hunter v Southam Inc* [1984] 2 SCR 145. See also *R v Dyment* [1988] 2 SCR 417, paras 15 and 30. Discussed in John D R Craig "Invasion of Privacy and Charter Values: The Common Law Tort Awakens" (1997) 42 McGill LJ 355.

471 Colin H H McNairn and Alexander K Scott *Privacy Law in Canada* (Butterworths, Markham (ON), 2001) 18-20.

472 *R v O'Connor* (1995) 130 DLR (4th) 235 (SCC).

473 *Aubry v Éditions Vice-Versa* [1998] 1 SCR 591. Decisions of the Supreme Court on appeal from Québec are not binding on the common-law provinces.

474 Privacy Act 1996 RSBC c 373 (British Columbia); Privacy Act CCSM s P125 (Manitoba); Privacy Act 1978 RSS c P-24 (Saskatchewan); Privacy Act 1990 RSNL c P-22 (Newfoundland and Labrador). For a general discussion of the Canadian torts, see also New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP 1, Sydney, 2007) 82-85. The British Columbia statute has recently been reviewed: British Columbia Law Institute *Report on the Privacy Act of British Columbia* (Vancouver, 2008).

475 Simon Chester, Jason Murphy and Eric Robb "Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?" (2003) 27 Advocates' Q 357, 373.

476 Civil Code of Québec RSQ 1991 c 64, ss 35-36.

The cause of action

4.120 The wording of each statute is very similar. They provide that "[it] is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person."[477] Manitoba provides that the violation must be "substantial, unreasonable and without claim of right."[478]

4.121 Each statute goes on to list examples of what may constitute a violation of privacy. These lists are non-exhaustive. They include:

- surveillance;
- listening to or recording of a conversation; and
- use of letters, diaries or other personal documents of a person.

Most provinces also include unauthorised use of the name, likeness or voice of a person in the list of examples of violations of privacy. However, British Columbia makes this a separate tort, in addition to the general one. The legislation provides that:[479]

> [it] is a tort, actionable without proof of damage, for a person to use the name or portrait of another for the purpose of advertising or promoting the sale of, or other trading in, property or services, unless that other, or a person entitled to consent on his or her behalf, consents to the use for that purpose.

4.122 Most provinces refer to the concept of reasonableness in some way. In British Columbia and Newfoundland, reasonableness is used to measure a person's entitlement to privacy. That is, the nature and degree of privacy to which a person is entitled is that which is reasonable in the circumstances, having regard to the lawful interests of others.[480] Conversely, in Manitoba unreasonableness on the part of the defendant is considered as an element in the conduct violating privacy.

4.123 It is notable that all the torts cover both disclosure of private information and intrusion. Thus, they protect both informational and spatial privacy. Also worth emphasising is that they do not require proof of damage.

Remedies

4.124 The remedies provided under each statute are essentially the same. Courts may:[481]

- award damages;
- grant an injunction;
- order the defendant to account to the plaintiff for any profits that have accrued, or that may subsequently accrue, to the defendant by reason or in consequence of the violation; and
- order the defendant to deliver up to the plaintiff all articles or documents that have come into his or her possession by reason or in consequence of the violation.

---

477 See, eg, Privacy Act 1978 RSS c P-24, s 2.

478 Privacy Act CCSM s P125, s 2(1).

479 Privacy Act 1996 RSBC c 373, s 3.

480 Privacy Act 1996 RSBC c 373, s 1(2); Privacy Act 1990 RSNL c P-22, s 3(2).

481 See, eg, Privacy Act CCSM s P125, s 4(1).

4.125 In awarding damages, courts must generally have regard to all the circumstances of the case including:[482]

- the nature, incidence and occasion of the act, conduct or publication constituting the violation of privacy of the person;
- the effect of the violation of privacy on the health, welfare, social, business or financial position of the person or his family;
- any relationship between the parties to the action;
- any distress, annoyance or embarrassment suffered by the person or his family arising from the violation of privacy; and
- the conduct of the person and the defendant, both before and after the commission of the violation of privacy, including any apology or offer of amends made by the defendant.

Defences

4.126 Again, each statute provides for similar defences. These include that the act or conduct complained of was:[483]

- consented to by the complainant or another person entitled to consent;
- incidental to the exercise of a lawful right of defence of person or property;
- authorised or required under a law in force in the province or by a court; or
- that of a peace officer or public officer engaged in an investigation in the course of his or her duties, and was neither disproportionate to the gravity of the matter under investigation nor committed in the course of a trespass.

Where publication is concerned, it is a defence that publication was reasonably believed to be in the public interest; was, under the law of defamation, privileged; or was fair comment on a matter of public interest. Manitoba adds a defence that the defendant did not know, nor reasonably should have known, that the relevant act violated privacy.[484] Notably, Saskatchewan provides a further defence that the violation of privacy was necessary for newsgathering and was reasonable in the circumstances.[485]

Experience of the torts

4.127 There have been very few actions under any of the statutes. A possible reason for the small amount of litigation is that actions can only be brought in the superior courts of the relevant province. Critics have suggested that this has made the action too costly and unduly restricted its availability.[486] Furthermore, plaintiffs often have not succeeded in litigation. In approximately

482 See, eg, Privacy Act CCSM s P125, s 4(2).

483 See, eg, Privacy Act 1990 RSNL c P-22, s 5.

484 Privacy Act CCSM s P125, s 5(b).

485 Privacy Act 1978 RSS c P-24, s 4(1)(e).

486 G H L Fridman *The Law of Torts in Canada* (2 ed, Carswell, Toronto, 2002) 710.

three out of every four cases, the defendant has successfully defended the action.[487] Where plaintiffs have succeeded, awards of damages have generally been very low.[488]

4.128 Fridman suggests that the courts have interpreted the statutes in a narrow way.[489] The following types of conduct have been found not to breach the relevant statute:

- a wife hiring a private investigator to track her husband, including installing a device in his car to track its location;[490]
- showing a topless photo of the plaintiff, which had been left in the defendant's jacket, to others;[491] and
- watching the plaintiff through a peephole in the wall of a cabin.[492]

4.129 Conversely, some examples of situations where plaintiffs have been successful are:

- an insurance company hiring an investigator to investigate a person against whom it had no legal claim;[493]
- newspapers inadvertently breaching name suppression orders relating to victims in sexual violence cases;[494]
- publication in the media of a video of the plaintiff without consent;[495] and
- a landlord secretly videotaping the plaintiff in her bathroom and bedroom.[496]

Common law torts

4.130 In the provinces without a statutory cause of action, the common law continues to govern privacy, and in some of these provinces there have been indications that the courts will develop a tort of invasion of privacy.[497] In addition, in some provinces with a statutory tort, the courts have indicated that they may develop the common law alongside statute.[498] However, the position is not yet clear.

487 Simon Chester, Jason Murphy and Eric Robb "Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?" (2003) 27 Advocates' Q 357, 365.

488 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 84.

489 G H L Fridman *The Law of Torts in Canada* (2 ed, Carswell, Toronto, 2002) 716.

490 *Davis v McArthur* (1969) 10 DLR (3d) 250 (BC CA).

491 *Milton v Savinkoff* (1993) 18 CCLT (2d) 288 (BC SC).

492 *Lee v Jacobson* (1994) 99 BCLR (2d) 144 (BC CA).

493 *Insurance Corp of British Columbia v Somosh* (1983) 51 BCLR 344 (BC SC).

494 *C (P R) v Canadian Newspaper Co* (1993) 16 CCLT (2d) 275 (BC SC); *F (J M) v Chappell* (1998) 158 DLR (4th) 430 (BC CA).

495 *Hollinsworth v BCTV* (1998) 113 BCLR (3d) 121 (BC CA).

496 *Malcolm v Fleming* (10 April 2000) BC SC, Doc No S17603, Downs J.

497 See generally G H L Fridman *The Law of Torts in Canada* (2 ed, Carswell, Toronto, 2002) ch 24.

498 See, eg, *R v Gill* [1995] 7 WWR 61 (Man QB).

4.131 In a number of lower-court cases, particularly in Ontario, judges have suggested that a cause of action for invasion of privacy might exist. However, the courts in these cases did not need to rely on privacy.[499] A number of more recent lower-court cases have in fact held that a cause of action exists. In one case, involving a boundary dispute between neighbours, one neighbour trained a surveillance camera on the other's yard. The court held that this was an intentional invasion of privacy and was actionable (although the claim was under the heads of trespass and nuisance).[500] In another case, telephone harassment was considered an invasion of privacy.[501]

4.132 It is notable, however, that no appellate court has recognised a common law tort of breach of privacy.[502] Furthermore, the most recent Ontario superior-court decision found that Canadian law has not clearly recognised invasion of privacy as a discrete tort. The Court suggested that there may be an "embryonic" tort, but that it would only apply where there is harassment or an intentional invasion of privacy.[503]

Privacy legislation

4.133 Canada has two Federal privacy laws. These are the Personal Information Protection and Electronic Documents Act 2000 (PIPEDA), which applies to the private sector, and the Privacy Act 1985, which applies to the public sector. Together these are broadly similar to New Zealand's Privacy Act 1993, and are based on a set of privacy principles which are similar to New Zealand's. Individuals can complain to the Privacy Commissioner of Canada about breaches of both Acts. The Commissioner has the power to take a case to the Federal Court, seeking an order to stop an organisation from doing a particular practice or for payment of damages.[504]

4.134 In addition, each province and territory has privacy legislation governing the collection, use and disclosure of personal information held by the public sector. British Columbia, Alberta and Québec also have legislation that is substantially similar to PIPEDA.[505]

4.135 There is also Federal and provincial legislation providing protection for privacy in certain specific areas. For example, the Telecommunications Act has as an objective "to contribute to the protection of the privacy of persons."[506] Federal banking legislation and provincial credit reporting laws also contain privacy

499 See, eg, *Burnett v R* (1979) 94 DLR (3d) 281 (Ont HC); *Capan v Capan* (1980) 14 CCLT 191 (Ont HC); *Saccone v Orr* (1981) 19 CCLT 37 (Ont Co Ct); *F(P) v Ontario* (1989) 47 CCLT 231 (Ont DC); *R v Otto* (1984) 16 CCC (3d) 289 (BC Co Ct). Discussed in G H L Fridman *The Law of Torts in Canada* (2 ed, Carswell, Toronto, 2002) 701-703.

500 *Lipiec v Borsa* (1996) 31 CCLT (2d) 294 (Ont Gen Div) paras 16-18.

501 *Provincial Partitions Inc v Ashcor Implant Structures Ltd* (1993) 50 CPR (3d) 497 (Ont Gen Div).

502 Russell Brown "Rethinking Privacy: Exclusivity, Private Relation and Tort Law" (2006) 43 Alta L Rev 589.

503 *Haskett v Trans Union of Canada* (2002) 10 CCLT (3d) 128 (Ont SC) paras 40-49.

504 Privacy Act RS 1985 c P-21; s 42; Personal Information Protection and Electronic Documents Act 2000 c 5, s16.

505 See generally Office of the Privacy Commissioner of Canada "Fact Sheet: Privacy Legislation in Canada" www.privcom.gc.ca (accessed 21 May 2008).

506 Telecommunications Act (Canada) SC 1993 C38, s 7(i).

provisions. Alberta, Saskatchewan, Manitoba and Ontario have specific legislation dealing with the collection, use and disclosure of personal health information.[507]

Regulation of the media

4.136 The Canadian Radio-television and Telecommunications Commission (CRTC) regulates and supervises broadcasting, as well as some aspects of telecommunications.[508] The majority of the CRTC's work involves licensing of broadcasters. It also encourages broadcasters to develop voluntary codes.[509] The Canadian Broadcast Standards Council (CBSC), a voluntary industry body covering many private broadcasters, develops codes and hears complaints against private broadcasters about breaches of codes. The code of journalistic ethics which it administers includes an article on privacy.[510] If the CBSC finds a breach of a code, it may require the broadcaster to announce that decision on air. Complainants who are unhappy with a CBSC decision may ask the CRTC to review the decision, in which case the CRTC considers the matter de novo.[511] The public broadcaster CBC also has a code of journalistic standards and practices which includes a section on privacy. Complaints about breaches of this code can be made to the CBC's Ombudsman.[512]

4.137 All provinces except Saskatchewan have a Press Council similar to New Zealand's.[513] There is no national body that regulates the press. Most Press Councils have standards or guidelines relating to privacy. For example, the British Columbia Press Council's Code of Practice provides that:[514]

> Newspapers should strive to balance an individual's desire for privacy with the requirements of a free press. Privacy concerns, therefore, must not unduly inhibit newspapers from publishing material or making inquiries about an individual's private life when it can be shown that these are, or are reasonably believed to be, in the public interest.

Criminal sanctions

4.138 Canada has enacted criminal laws covering certain areas of privacy. For example, there is an offence of criminal harassment.[515] One particular area covered is telecommunications and electronic surveillance. Part VI of the

507 Office of the Privacy Commissioner of Canada "Fact Sheet: Privacy Legislation in Canada" www.privcom.gc.ca (accessed 21 May 2008).

508 Canadian Radio-television and Telecommunications Commission "About the CRTC" www.crtc.gc.ca.eng (accessed 22 May 2008).

509 Robert Martin *Media Law* (2 ed, Irwin Law, Toronto, 2003) 17.

510 Radio Television News Directors Association of Canada Code of Ethics, art 4, www.cbsc.ca (accessed 11 December 2008).

511 Canadian Broadcast Standards Council "Questions Concerning CBSC Decisions" www.cbsc.ca (accessed 11 December 2008).

512 CBC/Radio-Canada "Media Accountability" http://cbc.radio-canada.ca (accessed 11 December 2008).

513 See generally "Press Council Directory" www.media-accountability.org (accessed 22 May 2008).

514 British Columbia Press Council "Code of Practice" www.bcpresscouncil.org (accessed 16 June 2008).

515 Criminal Code (Canada) RSC 1985 c C-46, s 264.

Criminal Code deals with invasion of privacy,[516] and contains provisions regulating electronic surveillance by government, private citizens and organisations. It prohibits the use of certain electronic devices to intercept private communications, as well as disclosure of information discovered through the use of these devices. However, the courts may authorise the interception of private communications. The Code also contains provisions protecting the privacy of computer users. It is an offence to fraudulently intercept any function of a computer system, and to use or traffic in another person's computer password.[517]

Conclusion

4.139 Canadian law protects privacy through a number of different channels, including statutory torts (and potentially a common law tort), specific privacy legislation, the Charter and, to some extent, the criminal law. Overall, as in most jurisdictions surveyed, the situation is something of a patchwork and the law does not provide a fully coherent framework of protection for privacy interests. The Canadian situation is interesting because it has statutory torts in place that protect both informational and spatial privacy. It also may have an emergent common law tort. But, as in the United States, plaintiffs have not had wide success with the actions.

516 Criminal Code (Canada) RSC 1985 c C-46, Part VI.

517 See generally Colin H H McNairn and Alexander K Scott *Privacy Law in Canada* (Butterworths, Markham (ON), 2001) Chapter 7.

Chapter 5

Conclusion on the current legal position

5.1 So far this paper has outlined the current law in New Zealand and other countries with which we compare ourselves. We have outlined various different methods of enforcement: criminal law and civil law, which are both enforced in the courts, and other enforcement mechanisms, which take place outside the courts. The complaints process under the Privacy Act 1993 and the Broadcasting Standards Authority are examples of the latter type. Some of the court processes developed before the other mechanisms existed.

5.2 This chapter draws some conclusions about the existing state of the law, identifies some gaps, anomalies and problems that we will consider for reform in later parts of this paper, and considers what we might learn from overseas.

ASSESSMENT OF NEW ZEALAND LAW

Criminal law

5.3 As we outlined in chapter 2, there is a miscellaneous array of criminal offences in New Zealand which impose penalties for various sorts of conduct that might be categorised as invasions of privacy. While the existing coverage of the criminal law is somewhat patchy, some broad categories are discernible. The law offers protection against intrusions such as peeping and peering into houses, photographing or filming people in intimate situations without their consent, trespass and harassment. Privacy of communications, especially via mail and telephone, receives fairly extensive protection. There are also many offences relating to disclosure of private or confidential information.

No rationale

5.4 However, it is not easy to discern a clear rationale for making certain invasions of privacy criminal, nor does the existing criminal law cover the entire range of possible privacy invasions.

5.5 As with the civil remedies, a question arises as to how many of the offences are really about protecting privacy: a number protect privacy only indirectly. For example, trespass is aimed at protecting property rights. However, because the concepts of privacy and property are linked, trespass also protects people's privacy in their homes. Some offences protect people other

than the person to whom the personal information in question relates. For example, the prohibition on publishing information obtained by Mortality Review Committees is probably meant to protect the feelings of the deceased person's family, although the deceased person's privacy may have also been a consideration.

5.6 Many of the offences described seem to protect a range of interests, mixing privacy with other unrelated concerns. For example, the prohibition on disclosure of tax information aims to protect the integrity of the taxation system and the government's ability to collect taxes. It also, by protecting information which citizens are required to supply, promotes trust in government. The offences relating to use and disclosure of electoral information are similar. They are probably mostly directed at preserving the integrity of elections, but protecting personal information is also important. In other instances, safety,[518] security,[519] financial interests[520] or reputation[521] are the prime concerns of some of the offences.

5.7 Our survey of criminal offences related to privacy also highlights the difficulty of separating privacy from related concepts such as secrecy and confidentiality. Secret information need not be personal information: for example business information can be secret. Confidentiality is closely related to privacy, but it is generally concerned with the circumstances in which information was acquired, whereas privacy is usually more concerned with the nature of the information.[522]

5.8 In some of the offences secrecy, confidentiality and privacy are closely intertwined. Examples are the offences relating to secrecy of tax information, statistics and information obtained by ombudsmen.

5.9 Likewise, the provisions relating to information collected as part of the National Cervical Screening Programme may be seen as protecting the confidentiality as well as the privacy of this information, as information would generally be given in the context of a doctor-patient relationship.

5.10 All this illustrates the wide range of interests which may be protected by provisions that we think of as privacy-related. Their diversity, and the range of policies which underlie them, must make us wary of apparently simple solutions.

---

518 The prohibition on publishing information provided to offenders by the Parole Board in a form that identifies the victim is probably primarily aimed at ensuring victims are safe, but also protects victims' privacy.

519 For example, the offences relating to: publishing information obtained by the NZSIS; postal services; and computer hacking.

520 For example, the offences relating to taxation information and the work of the Remuneration Authority.

521 For example, the provisions of the Criminal Records (Clean Slate) Act 2004.

522 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 48-51. In *Privacy: Concepts and Issues* we drew some distinctions between these concepts, but also noted that they can overlap considerably. We defined secrecy in terms of concealing or withholding information.

Anomalies

5.11 Some aspects of the criminal law seem anomalous. It is an offence to use a listening device to intercept a private conversation, but no offence to secretly film someone (unless the film is of an intimate nature). It is an offence to peep through a dwelling house window at night, but not during the day time. Sometimes there may be a rational basis for such differences. For example, it may be thought that intercepting a private conversation enables the collection of more personal information than simply filming someone's actions. However, it is worth considering whether the differences are justified. The penalties lack consistency too. Why should a peeping tom be liable only to a fine of $500, but a person who tape records someone's conversation to two years' imprisonment?

Difficulties with the criminal law

5.12 While sometimes the deterrent effect of the criminal law is needed, there can be difficulties with leaving things to be dealt with by the criminal law. The victim is generally reliant on the willingness of the Police to investigate and prosecute, since private prosecutions are rare and expensive. Furthermore, the criminal law is not directed at providing a remedy for the victim. We discuss the role of the criminal law in protecting privacy further below.

A more principled approach?

5.13 There is a question of whether a more principled approach can be adopted to the protection of privacy by the criminal law. In chapter 7 of this paper, which relates to information disclosure, and Part 3 relating to surveillance and intrusion, we examine whether changes to the existing criminal law are necessary in order to achieve this. This involves some deep and difficult questions about what the role of the criminal law is, or should be.

Civil Law

Civil remedies and informational privacy

5.14 Informational privacy receives fairly broad protection by the civil law. In some instances, this protection is indirect: actions for breach of confidence, defamation, malicious falsehood and breach of contract may all be called into aid to prevent private information being revealed, but it cannot be said that any of these remedies were developed with "privacy" specifically in mind.

5.15 In contrast, the *Hosking* tort provides a direct remedy against the disclosure of private facts about a person.[523] Yet, there are numerous uncertainties about the tort. It requires a court to make some fairly subjective judgments. People might easily disagree on whether in a particular case the facts were such as might reasonably be expected to be kept private; or whether it was highly offensive to publish them; or whether public concern overrides the privacy interest.

523 The Privacy Act 1993, Broadcasting Standards Authority and Press Council also provide further civil remedies against the misuse and disclosure of private information.

There will be cases where it will be quite hard to predict which way a court will go, and where it will therefore be difficult for lawyers to advise their clients. Such uncertainty can act as a restraint on freedom of expression.

5.16 Moreover, there are many gaps in the tort which remain to be resolved. Does it apply to corporations as well as individual human beings? Can a deceased person's family sue for breach of the deceased's privacy? If some of the statements made are untrue can you bring a privacy action in respect of those?

5.17 We discuss the tort further in chapters 6 and 7, and ask questions about its future development.

Civil remedies and spatial privacy

5.18 Spatial privacy is also given some indirect protection by the civil law, particularly under the Harassment Act 1997 and the tort of trespass to land. Thus, individuals may obtain some protection from the law if they are repeatedly pursued and observed, or if a person enters their land without invitation, to observe or record them. However, there is no direct remedy in the courts for intrusion into seclusion and solitude. The *Hosking* tort does not extend this far, although it may be that the courts will choose to apply it to spatial privacy in the future. Again, this is uncertain. In Part 3 of this paper, we describe the sorts of behaviours that might infringe upon spatial privacy and consider whether further civil remedies are needed. In particular, in chapter 11 we consider the possibility of a distinct intrusion tort.

Difficulties with civil remedies

5.19 Civil remedies have significant drawbacks. Civil actions in the courts are expensive and can involve considerable delay. Most ordinary citizens could not realistically afford to take an action. The possibility of having costs awarded against them would also be a significant disincentive. Thus, civil remedies are arguably the least accessible form of redress for breaches of privacy. There may be a valid concern that only the rich and famous will benefit.[524]

5.20 There are some particular problems with the use of civil actions in the courts to remedy breaches of privacy. Arguably, compensation is not an especially meaningful remedy because it cannot restore lost privacy, although it may have some value in providing incentives not to breach privacy at all. Conversely, civil action does have one significant advantage: injunctions can be awarded to stop breaches of privacy before they occur. Many of the claims that have been made under the tort of invasion of privacy have in fact been for injunctions.

5.21 Furthermore, in the privacy context there are particularly acute concerns around uncertainty. We have discussed the uncertainties in the *Hosking* tort. The application of the tort of breach of statutory duty is equally uncertain. This may act as a disincentive to bringing an action for breach of privacy, making the courts an even less accessible forum.

524 Although it must be noted that in New Zealand since 1985 some fifteen people have brought cases wholly or partly based on privacy, and many of them have been neither rich nor famous. Sometimes legal aid may be available.

5.22 Civil proceedings are also open to the public, meaning that people taking an action to prevent a breach of their privacy are forced to reveal private information in a public setting, which seems inconsistent with the very purpose of taking a claim to protect their privacy.

5.23 We need to ask, then, whether civil remedies are the best way to protect privacy in today's context, or whether some alternative system would be better. There is a general trend towards using alternative dispute resolution methods rather than using the courts as first recourse to settle disputes. Mechanisms such as ombudsmen are also increasingly used. The Privacy Act itself provides for conciliation and mediation by the Privacy Commissioner, with action in the Human Rights Review Tribunal only if the Commissioner is unable to resolve the complaint. It may be that the rest of privacy law should align with this trend. Alternatives to the courts can of course be used alongside the courts: for example, mediation with the option of court action in the event of failure.

Other "regulatory" enforcement schemes

5.24 Complaints schemes under the Privacy Act 1993, and those run by the various media regulation bodies (Broadcasting Standards Authority, Press Council and Advertising Standards Authority) provide easy access to complaints mechanisms for some privacy invasions. Pursuing complaints through these bodies is likely to be much cheaper and quicker than pursuing a civil claim through the general court system. The mechanisms carry other benefits: for example, the Privacy Act and BSA principles and case law give fairly specific direction about the forms of privacy intrusion protected. Another important advantage is that a complaints body such as the Privacy Commissioner can address systemic issues. They can work with agencies to help improve their systems so that privacy breaches are less likely to occur.

5.25 However, again gaps exist. The Privacy Act provides for complaints to the Privacy Commissioner, and potentially action in the Human Rights Review Tribunal, in relation to breaches of information privacy principles, Codes of Practice and information-matching rules. Most notably, the Act does not apply to the news media in relation to their news activities. Also, for the most part the Act is not directed at protection against forms of invasion of privacy other than informational privacy, such as surveillance or intrusion into solitude and seclusion. However, principles 3 and 4 do potentially apply to some surveillance activities.

5.26 The BSA, Press Council and ASA receive complaints about breaches of privacy by the media and advertisers. Their privacy principles do cover a broad range of types of privacy, not only privacy of personal information (although the ASA's privacy rule is quite limited). In particular, the BSA has developed fairly comprehensive jurisprudence relating to intrusion. However, the remedies these bodies can award are more limited than the remedies available under the Privacy Act or tort remedies. The Press Council cannot impose any sanction, although the print media have voluntarily agreed to publish decisions adverse to them, and the ASA can only ask the advertiser to withdraw the advertisement. The BSA can award damages of up to $5000 and imposes sanctions such as taking a station off the air or banning advertising for a period. It can also award costs.

5.27 Therefore, while the available complaint mechanisms cover many invasions of privacy, the coverage is, again, incomplete. In particular, except in relation to complaints against media, there is currently no comprehensive mechanism to remedy invasions of privacy such as surveillance and intrusion into solitude and seclusion. Regulation of the print media is also fairly light-handed, with little sanction for invasion of privacy. Another gap is that there is currently no regulation of forms of media other than broadcast and print media. The internet, most significantly, and other new media are largely unregulated.

5.28 A key drawback of all of the lower-level mechanisms is that they cannot prevent a breach of privacy before it occurs. In contrast, the courts can issue an injunction. This is the major attraction of the courts for many. Arguably the ability to get an injunction is especially important in privacy, as once a breach of privacy has occurred the damage has been done. Compensation is a poor substitute for the lost privacy. However, injunctions have a significant impact on freedom of expression, as they prevent expression before it happens rather than imposing penalties after the event.

Overall assessment of privacy protection in New Zealand

5.29 New Zealand law offers some protection for privacy interests. However, the law is piecemeal and there are some significant gaps and anomalies.

5.30 A key gap that we see is that surveillance and intrusion are not comprehensively covered by any of the current modes of enforcement. It is uncertain whether the tort covers intrusion, the criminal law is patchy, the BSA, Press Council and ASA can only act where there is publication, and it is not clear to what extent surveillance and intrusion are covered by the Privacy Act. There is a mismatch between legal controls on surveillance by law enforcement agencies and those covering private individuals.

5.31 For some invasions of privacy there are heavy penalties (for example, intimate covert filming and interception of private communications), for some there are light penalties (for example, peeping and peering), for some there are none at all (for example, covert filming of a non-intimate nature). Furthermore, it may be questioned whether some invasions of privacy, which are currently criminal offences, truly merit the use of criminal penalties.

5.32 In some areas the law is uncertain and vague. This is especially so for the tort remedies. In part this flows from the uncertainty in the very concept of privacy. For example, "reasonable expectation of privacy" cannot be defined precisely, but rather will always require a contextual assessment. Case law will take time to clarify these uncertainties.

5.33 It is not clear that the current law is able to keep pace with technological developments. The internet in particular poses privacy challenges. As we discuss further in Part 3, advances in surveillance technology are making surveillance more widespread, so the need to fill the gap in this area of the law becomes more urgent.

5.34 Some of the mechanisms for enforcement are more easily accessible than others. Complaints to the Privacy Commissioner and to media regulatory bodies such as the BSA are cheap and relatively speedy, but the remedies that can be awarded through these channels are limited and their coverage is confined to certain areas. In contrast, the courts can award greater remedies but are beyond the reach of some sectors of society.

5.35 Finally, it is not clear that the balance between competing interests is always right. Public interest or public concern is a defence to the privacy tort and with the BSA and Press Council, but not in the case of many of the criminal offences, nor some of the specific torts. The Privacy Act, rather than using the concept of public interest, specifies detailed exceptions to each principle, many of which are designed to protect the public interest. The Act also addresses the balance between privacy and competing interests in section 14, which requires the Privacy Commissioner to have due regard for the protection of important human rights and social interests that compete with privacy.

WHAT CAN WE LEARN FROM OVERSEAS?

5.36 The overseas countries we have looked at have many similarities to New Zealand. Most countries have a somewhat patchy legal framework for privacy protection: most have data protection legislation broadly based on the OECD principles, a variety of criminal offences without much rationale and some media regulation which tends to be fairly light-handed and not comprehensive. Some have tort remedies, either in common law or statutory form.

5.37 We ought to be careful of relying too much on overseas models: the constitutional arrangements elsewhere, particularly in the United States and the United Kingdom, are different to New Zealand's. That said, one notable difference is that, in many countries that have a tort, the tort covers intrusion as well as disclosure of private information. This is the case in the United States and in those Canadian provinces with a statutory tort, and has also been proposed by the Australian Law Reform Commission. In this respect, these torts offer more comprehensive protection than the *Hosking* tort as it currently stands.

5.38 Attempts at statutory reform overseas have had limited success. Proposed statutory torts (covering both intrusion and publicity) in both Hong Kong and Ireland were not enacted. There has also been strong media opposition to the recent Australian Law Reform Commission proposals to enact a statutory tort. Similarly, attempts in New South Wales, Ireland and Hong Kong to regulate surveillance in a comprehensive way have been unsuccessful.[525]

5.39 Similarly, torts of invasion of privacy, under common law in the United States and statute in Canada, have not been especially successful. There have been comparatively few cases in both countries and plaintiffs have tended not to succeed often. However, the United States in particular has a different constitutional context, so the experience in New Zealand may not necessarily be the same. Success rates have been higher in England.

5.40 All this illustrates that reform is not straightforward. Freedom of action and expression are powerful countervailing influences against increased privacy protections. Strong voices are raised in support of extreme positions at both ends

525 We discuss the detail of these proposals in chapter 10.

of the scale. However, again overseas experience should not necessarily be taken to mean that reform is impossible in New Zealand, nor that reform is not desirable.

WHERE TO FROM HERE?

5.41 Based on our analysis of the existing law in Part 1, in Parts 2 and 3 of this paper we examine potential reforms under the headings of information disclosure (Part 2) and intrusion (Part 3). Potential reforms involve a mix of criminal law, civil law and other regulatory options. Therefore, before considering the options it is useful to attempt to define some principles regarding the appropriate spheres of various options.

Roles of the civil and criminal law

5.42 In general, criminal penalties have been associated with public interests and civil remedies with private interests. The civil law is generally concerned with compensating individuals for harm they have suffered and is generally not concerned with punishing the person who caused the harm.[526] Conversely, the criminal law is concerned with vindicating societal interests by punishing offenders,[527] and with deterring potential future offenders. Criminal penalties carry a certain social stigma, acting as a mark of society's disapproval of the offence, so are often seen as the more serious. It is sometimes said that criminal offences are in respect of conduct so grave that it should be prosecuted by the state, whereas breaches of the civil law are not so grave, so can be left to individuals to deal with. In general, the criminal law would not be used if the civil law is sufficient to keep the relevant conduct in check.[528]

5.43 The distinction between criminal and civil law is not so clear-cut, however, as this suggests. There are criminal sentences that involve compensating the victim for harm suffered, for example.[529] Recent developments such as the increasing use of civil penalties imposed by the state,[530] as well as the expanding use of the criminal law to regulate areas such as business or the environment,[531] have further blurred the distinction.

5.44 It is also important to note that the criminal and civil law can be used alongside each other, with criminal penalties allowing the offender to be punished and civil remedies to compensate the individual harm.[532] Many crimes are torts as well.

526 Stephen Todd "General Introduction" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 1, 3.

527 John G Fleming *The Law of Torts* (9 ed, LBC Information Services, North Ryde (NSW), 1998) 3-4; Australian Law Reform Commission *Principled Regulation: Federal Civil & Administrative Penalties in Australia* (ALRC R95, Sydney, 2002) 2.15.

528 Glanville Williams *Textbook of Criminal Law* (2 ed, Stevens and Sons, London, 1983) 33.

529 See, eg, Sentencing Act 2002, s 12.

530 Some examples of civil penalties in New Zealand are fines under the Fisheries Act 1996 for failure to comply with standards and specifications, fines under the Commerce Act 1986 for contravention of a cease and desist order and fines for contravention of the Takeovers Act 1993 or the Takeovers Code.

531 An example of this type of criminal offence is found in the Resource Management Act 1993. Section 338 sets out a number of offences, such as discharging harmful substances or contaminants in the coastal marine area in contravention of the Act.

532 See, eg, Harrassment Act 1997, which includes both a civil and a criminal regime, although it does not make provision for compensation.

Practical considerations

5.45 In reality, the decision whether certain conduct ought to be regulated by the civil or criminal law often involves practical decisions based on the powers and procedures associated with each. Advantages of choosing civil proceedings are that the standard of proof is lower, and civil court procedures facilitate evidence gathering. In addition, remedies such as damages and injunctions are available. Conversely, the key advantage of the criminal law is that police powers of arrest, detection and investigation become available in relation to the conduct. Importantly, the power to arrest means that the police can intervene immediately, whereas taking civil proceedings can involve considerable delay. The criminal law arguably has greater deterrent value. It also allows for deterrent and incapacitative penalties, such as prison or rehabilitative sentences.[533]

5.46 Who can institute proceedings is also a relevant practical consideration. The Police can bring criminal proceedings to protect the public where there is no one who can be relied on to take civil proceedings.[534]

5.47 A related consideration is cost. The criminal law has the advantage that it is enforced by the state and the state meets the direct costs of investigation and prosecution. Conversely, the civil law relies on individuals to take often costly court action against those who have harmed them.

5.48 An example of how these types of considerations can influence decisions about whether to criminalise certain conduct can be found in the Law Commission's consideration of intimate covert filming. The Commission considered that there should be a criminal offence because of the exploitative and sexual nature of the conduct, its potential links to more serious criminal offending, the significance of the invasion of privacy involved and its wider societal implications, the fact that Police could intervene to stop the filming as it occurred, the fact that filming might be difficult for individuals to detect and investigate themselves, so Police detection and investigation powers would be useful, and the fact that criminal penalties were considered appropriate. It also recommended that the Privacy Act should be amended to provide a civil remedy.[535]

Principles

When should the criminal law be used?

5.49 The Legislation Advisory Committee Guidelines suggest that the following questions should be used to guide the assessment of whether particular conduct is suitable for criminal sanctions:[536]

- Will the conduct, if permitted or allowed to continue, cause substantial harm to individual or public interests?
- Would public opinion support the use of the criminal law, or is the conduct

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

534 Glanville Williams *Textbook of Criminal Law* (2 ed, Stevens and Sons, London, 1983) 33.

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

536 Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2001) para 12.1.3.

in question likely to be regarded as trivial by the public?

- Is the conduct in question best regulated by the civil law because the appropriate remedies are those characteristic of the civil law (for example, compensation or restitution)?
- Is the use of the criminal law being considered solely or primarily for reasons of convenience rather than as a consequence of a decision that the conduct itself warrants criminal sanctions?
- If the conduct in question is made a criminal offence, how will enforcement be undertaken, who will be responsible for the investigation and prosecution of the offence, and what powers will be required for enforcement to be undertaken?

Given the difficulties inherent in defining what is properly within the scope of the criminal law, we think that the above guidelines express the key considerations in determining which types of conduct ought to be criminal.

When should the civil law be used?

5.50 Similar considerations, but in reverse, will guide the assessment of whether the civil law is appropriate in a particular context. That is, the civil law should be used where the primary interest is to compensate individuals rather than vindicate public interests, where the public would not support the use of the criminal law and where civil remedies are the appropriate remedies. Sometimes it will be entirely appropriate that the same conduct should attract both criminal and civil sanctions.

When should other forms of regulation be used?

5.51 Regulatory systems through which people can receive redress outside the courts can be used to avoid some of the drawbacks of civil action in the courts, which we have discussed. We have in mind here complaints processes such as those under the Privacy Act, as well as other alternatives to the courts, such as tribunals. These dispute-resolution mechanisms have many advantages: they are cost-effective, quick, and generally simpler and less formal than the courts. They therefore tend to be more easily accessible to the general public than the courts. Specialist expertise is another key advantage of these types of processes as opposed to the ordinary courts, which are generalist.[537]

5.52 The following types of considerations are relevant in assessing whether an alternative dispute resolution process to the courts should be used:[538]

- cost;
- speed;
- the importance of specialist expertise;
- the need for a less formal approach than that of the courts;
- the desirability of different fact-finding procedures to those of the courts;

537 See, eg, New Zealand Law Commission *Tribunals in New Zealand* (NZLC IP6, Wellington, 2008) paras 2.27-2.34.

538 Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2007) 388 and para 11.3.2; New Zealand Law Commission *Tribunals in New Zealand* (NZLC IP6, Wellington, 2008) paras 2.27-2.34.

- the need to allow for mediation or other forms of dispute resolution not available through the courts;
- the desirability of encouraging a co-operative approach; and
- the need for confidentiality.

Self-regulation

5.53 In some cases it may be best for industries or groups to regulate themselves. The Ministry of Consumer Affairs has identified the following situations where self-regulation may be the best option:[539]

- government regulation is unlikely to occur or is inappropriate;
- overarching legislation already exists and the objective of self-regulation is to assist or promote compliance with the legislation within a particular sector;
- there is widespread acknowledgment within a sector or group of the need for, and commitment to, the development of regulatory controls; or
- the objective is to provide benefits beyond the minimum standards required by law.

Self-regulation may also be useful where it is desirable for groups to have a sense of "ownership" of the rules, or where a more flexible approach than that available through legislative intervention is required.[540]

Combining different enforcement mechanisms

5.54 An approach to regulating privacy will probably involve a mixture of enforcement mechanisms, using criminal law, civil law, regulatory systems and possibly some elements of self-regulation.

CONCLUSION

5.55 In Part 1 of this paper, we have set out the existing law in New Zealand and other countries. We have identified problems, gaps and anomalies in the existing law. This chapter provides a basis for our consideration of potential reforms.

5.56 The rest of this paper proceeds to discuss potential reform under the headings of information disclosure and intrusion, while recognising that in some cases the distinction between the two will not be apt or easy to draw.

539 Ministry of Consumer Affairs *Market Self-Regulation and Codes of Practice* (Policy Paper, 1997) 6.

540 Ministry of Consumer Affairs *Market Self-Regulation and Codes of Practice* (Policy Paper, 1997) 7-8.

Part 2

DISCLOSURE OF PERSONAL INFORMATION

Chapter 6

The nature of the *Hosking* tort

6.1 In *Hosking v Runting*,[541] the New Zealand Court of Appeal by a majority of three to two decided that, as a matter of common law, there is in this country a tort of invasion of privacy by publicity given to private facts. The Court went to the heart of the matter and endorsed a separate tort rather than taking the route of breach of confidence. However, it may well be that the last word has not yet been spoken. The Supreme Court is, of course, not bound by the Court of Appeal. In *Rogers v Television New Zealand*,[542] the parties accepted that the law was as stated in the majority judgments in *Hosking* so it was unnecessary for the Supreme Court to pronounce on the matter. However, Elias CJ was not prepared to accept that the limits of the tort of privacy were those stated in the majority opinions in *Hosking*. In particular, she reserved her position on whether it should be a requirement that publication be highly offensive.[543] Anderson J, who had been one of the dissenters in the Court of Appeal in *Hosking,* said he did not wish to be taken as endorsing the law as elucidated by the majority of the Court of Appeal in that case:[544]

> It was decided by a bare majority and both the existence of the tort, and the scope of it if it continues to be recognised, will fall to be reviewed by this Court in an appropriate case.

6.2 For the purposes of this issues paper we shall assume that the New Zealand law is currently as it was enunciated in the majority judgments in *Hosking v Runting.* In this chapter we shall analyse the elements of the tort, and point out the uncertainties in its application and the areas where further elucidation is required. In an appendix to the chapter we list the cases, both before and after *Hosking*, where the privacy tort was an ingredient of the cause of action.

ITS BASIS

6.3 In the extensive literature on privacy, a number of reasons have been advanced as to why privacy should be protected. Among them are that it is essential for the development of relationships, and that it protects and enhances liberty of thought

541 [2005] 1 NZLR 1. See also discussion in chapter 2.

542 [2008] 2 NZLR 78.

543 *Rogers v Television New Zealand* [2008] 2 NZLR 78, para 25.

544 *Rogers v Television New Zealand* [2008] 2 NZLR 78, para 144.

and action. However, in the decided cases it is "autonomy" and "dignity" that have been mainly cited as the values that privacy protects. Both Lord Hoffmann in *Campbell*[545] and Tipping J in *Hosking*[546] referred to these values.

6.4 Neither autonomy nor dignity admits of precise definition. Both are protean concepts. Christopher McCrudden described "dignity" as:[547]

> Context-specific, varying significantly from jurisdiction to jurisdiction and (often) over time within particular jurisdictions. Indeed, instead of providing a basis for principled decision-making, dignity seems open to significant judicial manipulation, increasing rather than decreasing judicial discretion.

6.5 However, the standard dictionary definitions adequately enough convey what the two words mean. Autonomy connotes freedom of action and choice, and dignity is about being worthy of honour and respect. The two are linked. That was the philosopher Immanuel Kant's thesis, and David Feldman agrees:[548]

> The notion of autonomy is linked to that of dignity … One aspect of dignity is self respect … Dignity also encompasses a desire to be esteemed by others according to the standards of which we approve. These attributes make it possible and worthwhile for people to regard their own choices as important, and this is, in turn, a necessary condition for the exercise of autonomy.

6.6 Hans Nieuwenhuis argues that dignity has two aspects: on the one hand honour, respectability and status, and on the other "the enlightenment idea of (human) dignity conceived of as personal autonomy."[549] In this view, dignity is wider than autonomy, and includes it. It is a view which has been echoed elsewhere.[550] There is considerable support for the view that dignity in this wide sense is the principal basis for the new tort. Nicole Moreham has

545 *Campbell v MGN Ltd* [2004] 2 AC 457, para 51.

546 [2005] 1 NZLR 1, para 239. One of the earliest attempts to link privacy with dignity is Edward J Bloustein "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 NYULR 962.

547 Christopher McCrudden "Human Dignity and Judicial Interpretation of Human Rights" (2008) 19 EJIL 655.

548 David Feldman "Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty" (1994) 47 CLP 41, 54.

549 Hans Nieuwenhuis "The Core Business of Privacy Law: Protecting Autonomy" in Katja S Ziegler (ed) *Human Rights and Private Law: Privacy as Autonomy* (Hart Publishing, Oxford, 2007) 15, 17.

550 See, eg, Rohan J Hardcastle *Law and the Human Body* (Hart Publishing, Oxford, 2007) 17: "Autonomy is an aspect of the broader concept of human dignity. Following this view, the protection of autonomy can also be seen as the protection of human dignity." See also Human Genetics Commission (UK) *Inside Information: Balancing Interests in the Use of Personal Genetic Data* (Department of Health, London, 2002) 39: "The principle of respect for persons requires that we acknowledge the dignity of others and that we treat them as ends in themselves and not merely instrumentally as means to ends or objectives chosen by others. This means that we must respect the autonomy of others."

collected the authorities in a recent article.[551] A number of them refer to invasion of privacy as a "dignitary tort". In the *Brooker* case, Thomas J said that privacy was closely aligned to the dignity and worth of the human person.[552]

6.7 The concept of dignity in law goes back a long way: trespass to the person, for example, has often been described as a dignitary tort. However, dignity as a value in law received impetus from the Universal Declaration of Human Rights in 1948, article 1 of which states that "All human beings are born free and equal in dignity and rights." From that time the concept has steadily migrated into our domestic legal system. It appears expressly in the Privacy Act 1993, the New Zealand Bill of Rights Act 1990 and the Employment Relations Act 2000. To use the words of Justice Hammond, "It is now centre-stage."[553] Justice Baragwanath has called it "the core value, indeed the fundamental value, of a civilised society."[554]

6.8 This commonly-asserted relationship of privacy and dignity raises some questions.

6.9 First, it is not clear that dignity is the only interest protected by privacy. When we look at the damage which a privacy action might address there is a range going well beyond damage to dignity. The disclosure of sensitive personal information in a way which causes humiliation and distress is no doubt the quintessential example of the *Hosking* tort. But there is little doubt that financial loss could also be recoverable: if the details of my bank account were to be published, I could surely claim any loss resulting from an ensuing theft. My financial interest is at stake just as much as my dignity. Likewise, when a policeman who had shot a man in the course of duty was granted an injunction preventing disclosure of his new identity and whereabouts, the injunction was based on the tort of privacy,[555] but it was the officer's personal safety and that of his family which were at stake rather than just his dignity. When Max Mosley recovered damages for disclosure of his private sexual conduct, his reputation was every bit as much an issue as his dignity, although the latter was certainly involved also.[556] When Catherine Zeta-Jones and Michael Douglas had unauthorised photographs of their wedding published they recovered damages for, among other things, "the cost and inconvenience" of having to select authorised photographs for publication in a competing magazine.[557]

551 NA Moreham "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation: Essays in Honour of John Burrows QC* (LexisNexis NZ, Wellington, 2008) 231.

552 *Brooker v Police* [2007] 3 NZLR 91, para 251.

553 Hon Grant Hammond "Beyond Dignity" (Paper presented to International Symposium on the Law of Remedies, Auckland, 16 November 2007) 8. This paper is a comprehensive examination of the origins and implications of dignity as a legal value. See also David Feldman "Human Dignity as a Legal Value Part I" [1999] PL 682; Part II [2000] PL 61; A Gerwith "Dignity as the Basis of Rights" in Michael J Meyer and William A Parent (eds) *The Constitution of Rights, Human Dignity and American Values* (Cornell University Press, Ithaca (NY), 1992).

554 *R v Wharewaka* [2005] NZAR 606, para 26.

555 *Abbott v The Press* (13 December 2002) HC CHCH T9-02.

556 *Mosley v News Group Newspaper Ltd* [2008] EWHC 1777 (QB).

557 *Hello! Ltd v Douglas* [2006] QB 125.

6.10 The Privacy Act 1993 acknowledges that several interests can be at stake when a person's privacy is infringed.[558] In addition to "significant loss of dignity" it lists other types of recoverable loss, including adverse "effects on rights, benefits or interests." Privacy is a multifaceted concept.

6.11 Secondly, even when dignity is an issue, there are some questions as to how one values damage to it. The usual damage will be humiliation, distress and hurt feelings. Our courts are not yet much experienced in this exercise. Such damage is intangible and the valuation of it can be a matter of impression. In England, with one exception, the damages so far awarded for breach of confidence or privacy have tended to be low. Naomi Campbell received only £3500,[559] and Catherine Zeta-Jones and Michael Douglas £3750 each,[560] for the distress caused by the publication. In *Archer v Williams*, Jackson J said that damages for injury to feelings should normally be "kept to a modest level".[561] The exceptional case is *Mosley v News Group Newspapers Ltd*,[562] where Mosley was awarded £60,000 for disclosure in a newspaper of details of certain sexual practices. In New Zealand, in *Attorney-General v Brown*,[563] Brown was awarded $25,000 for a breach of privacy which had caused him much distress in the form of verbal and even physical abuse. Justice Hammond demonstrates that the tendency has also been towards conservative awards in other areas where dignity is in question: damages under the Employment Relations Act and the Bill of Rights Act, for example. His Honour believes that we require a more considered approach than exists at the moment. He has put it this way:[564]

> As I have suggested, one of the real difficulties in the way of corrective justice in relation to "dignitary wrongs", is that compensation necessarily turns on what we are supposed to be compensating for. If we respond with phrases like, the "indignity" or the "humiliation" of being treated in [that way], we lack benchmarks against which remedial figures can be set, other than "other cases". What is more, "other cases" might themselves simply represent the impressionistic behaviour of judges in those other cases: it could, at worst, be a case of the blind leading the blind.

Later in this chapter we consider whether, in a possible statutory formulation of the tort, some guidelines might be set in this matter.

558 Privacy Act 1993, s 66(1)(b). See also s 88 providing that damages lie for, among other things, pecuniary loss.

559 *Campbell v MGN Ltd* [2004] 2 AC 457, para 10.

560 *Hello! Ltd v Douglas* [2006] QB 125, para 25.

561 *Archer v Williams* [2003] EMLR 869, para 76.

562 [2008] EWHC 1777 (QB).

563 [2006] DCR 630.

564 Hon Grant Hammond "Beyond Dignity" (Paper presented to International Symposium on the Law of Remedies, Auckland, 16 November 2007) 33.

6.12 Thirdly, if privacy is indeed a dignitary tort, an argument might be mounted that it should be actionable without proof of damage. In New Zealand Nicole Moreham has so argued. If other invasions of our human dignity such as assault, battery and false imprisonment do not require proof of damage, why should privacy? Moreham proposes that:[565]

> If, as Bloustein has argued, a person whose privacy is breached suffers a similar indignity to someone who is kissed, pushed, punched, or locked up against his or her wishes then, like those plaintiffs [in trespass to the person cases], he or she should be able to vindicate that dignitary interest as a matter of right.

6.13 This links with the question of whether, to succeed in the tort in New Zealand, the plaintiff needs to prove highly offensive publication. Moreham argues that once it is acknowledged that privacy is a dignitary tort, it follows that the "highly offensive" requirement disappears.[566]

6.14 Fourthly, does privacy apply to non-human actors, such as corporations? Does it apply to deceased persons? As we demonstrated in our study paper on privacy, there remains a question of whether corporations or the next of kin of a deceased person can be beneficiaries of the new tort.[567] If dignity, a supremely personal virtue, is the basis of the tort, it would suggest that corporations are not covered. But "dignity" is more appropriately used with regard to deceased persons, so the question there may still be an open one.

6.15 Fifthly, invasion of privacy is only one way in which dignity can be affronted. If the common law can create a tort to protect our privacy, might it not also be prepared to declare tortious other kinds of offence to dignity? In England the Court of Appeal came close to declaring harassment to be a tort,[568] although that opening now seems to have been closed off by the House of Lords.[569] Could it be that such things as abuse or discrimination on grounds of race, religious belief or disability might be the subject of a tort action? Some of these things are addressed in a different way under the Human Rights Act 1993, but the common law is not beyond creating causes of action in parallel to statute. Some of the states in the United States even know a tort of "outrage", the abuse of a person in such a way as to humiliate them. If, as Justice Hammond says, dignity is moving to centre stage in the legal system, might it be that privacy is merely the first step? How wide are we opening the door, and where will it lead? Could we even some day see the merger of invasion of privacy with defamation into some kind of tort of "harm to dignity"? There might, and indeed should, be some nervousness about that as an end goal.

---

565 NA Moreham "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation: Essays in Honour of John Burrows QC* (LexisNexis NZ, Wellington, 2008) 231, 244, citing Edward J Bloustein "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 NYULR 962, 1002.

566 NA Moreham "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation: Essays in Honour of John Burrows QC* (LexisNexis NZ, Wellington, 2008) 231.

567 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 191-195.

568 *Khorasandjian v Bush* [1993] QB 727.

569 *Hunter v Canary Wharf Ltd* [1997] AC 655.

THE RELATIONSHIP WITH BREACH OF CONFIDENCE

6.16 The English approach, initially at least, was to employ breach of confidence as a surrogate for a privacy tort.[570] This has involved doing a degree of violence to the usually-accepted paradigm of breach of confidence as based on a relationship between two or more people. The classic instance of breach of confidence is where one person entrusts another with information on the understanding, express or implied, that it is confidential and will go no further.

6.17 Yet the truth is that breach of confidence was never exclusively based on the existence of a relationship of confidence. From an early time there were cases where the obligation of confidence was imposed because the information had been obtained in an unlawful or surreptitious way – by theft, for instance.[571] That mode of acquisition was enough to impose a burden on the recipient's conscience. It is perhaps not a far cry to move from that point to cases where there has been surreptitious photography.[572] The English courts have now arrived at the point where they are prepared to impose an obligation of confidence in the absence of any relationship of confidence, or any surreptitious mode of acquisition, simply because the information, however obtained, is of an obviously private nature. In the latter case they are prepared to hold that even a person who has innocently received such information should realise from its nature that it was not meant for publication. Already questions have been raised by some Judges in England whether in cases of that kind the label "breach of confidence" is appropriate. Lord Nicholls, for example, would prefer to describe the cause of action simply as "misuse of private information."[573]

6.18 In *Hosking v Runting* at first instance,[574] Randerson J was prepared to allow the law to develop by extension of breach of confidence rather than acknowledge the existence of a separate tort of invasion of privacy. However, now the Court of Appeal in *Hosking v Runting* has decided that it is better to cut privacy loose from breach of confidence and establish a new free-standing tort. That approach avoids a cumbersome fiction and goes directly to the heart of the matter. Yet what is not absolutely clear from *Hosking* is the role which the Judges would now have breach of confidence play. Tipping J[575] and Keith J (dissenting)[576] appear to regard it as being confined to cases where a *relationship* of confidence exists. The others are not so emphatic about this.[577] The relationship between the two causes of action is thus not resolved by the case, and remains problematic at common law.

---

570 See chapter 4 above, and John Burrows "Invasion of Privacy" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 743, 751-754. Note also *Giller v Procopets* [2008] VSCA 236, where the Court of Appeal of the Supreme Court of Victoria used breach of confidence rather than relying on a separate privacy tort.

571 Stephen Todd "Interference with Intellectual Property" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 575, 616.

572 Lord Scott of Foscote "Confidentiality" in Jack Beetson and Yvonne Cripps (eds) *Freedom of Expression and Freedom of Information* (Oxford University Press, Oxford, 2000) 267.

573 *Campbell v MGN Ltd* [2004] 2 AC 457, para 14. It is notable that more recent English cases do not make as much reference to breach of confidence: they go directly to the question of whether the privacy protections in the European Convention are engaged. See, eg, *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 466.

574 [2003] 3 NZLR 385.

575 *Hosking v Runting* [2005] 1 NZLR 1, para 245.

576 *Hosking v Runting* [2005] 1 NZLR 1, para 201.

577 See especially *Hosking v Runting* [2005] 1 NZLR 1, para 49 Gault P and Blanchard J.

6.19 In many cases there will no doubt be the possibility of alternative causes of action. The facts of some of the leading English cases are good examples. Some of them involve personal confidences between domestic partners or friends,[578] some involve personal information acquired by the employee of the plaintiff while in an employment relationship.[579] In these cases the existence of the relationship means that an action for breach of confidence is entirely appropriate. In New Zealand the private nature of the information thus confided means that there would likely be a cause of action in the tort of invasion of privacy as well.[580] The plaintiff would thus have a choice, and might even sue on both in the alternative. This causes no particular problem. Alternative causes of action are familiar in our court system.

6.20 More difficult however, is the question of corporations. If, as appears likely, it is held that corporations cannot sue in invasion of privacy, the question will arise as to the situations in which they can claim in breach of confidence. That may raise the question of whether a relationship of confidence is necessary. The now famous conundrum posed by Lord Goff[581] is relevant: what if a reporter finds in a public street a piece of paper which has been wafted out of the window by a fan, and which contains obviously confidential information? There is here no relationship of confidence, nor any impropriety on the part of the reporter. The document has come into his or her hands by chance. Will an action for breach of confidence lie if the reporter discloses the information to the world? It is in a case of this kind that the exact boundaries of the law of breach of confidence will fall to be determined.

6.21 There are other questions, too, about the relationship between privacy and confidence:

- The interests protected by breach of confidence can range wide and cover all manner of commercial interests: trade secrets, for instance. It is not so clear to what extent the tort of invasion of privacy can provide redress in the commercial setting.
- Invasion of privacy, at least in the Gault-Blanchard formulation, protects only where there is highly offensive publication. Breach of confidence does not require that element.
- While identification of the plaintiff is probably necessary to ground an action in privacy, it is not so clear that it is required in breach of confidence.[582] It is possible to envisage an express obligation of confidence which extends so wide as to protect information irrespective of its connection with the person who confided it.

Whatever reforms are, or are not, made to the tort, there is likely to remain an awkward interface with breach of confidence. Any recommendations the Commission eventually makes are unlikely to resolve it.

578 See, eg, *Stephens v Avery* [1988] Ch 449.

579 See, eg, *Archer v Williams* [2003] EMLR 869.

580 In *Brown v Attorney-General* [2006] DCR 630, para 97 Judge Spear noted that action would have lain in both privacy and breach of confidence.

581 *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 281.

582 *Hosking v Runting* [2005] 1 NZLR 1, para 84 Gault P and Blanchard J.

THE ELEMENTS OF THE TORT: THE UNCERTAINTIES

6.22 In *Hosking* the elements of the tort were thus stated by Gault P and Blanchard J:[583]

> In this jurisdiction it can be said that there are two fundamental requirements for a successful claim for interference with privacy:
>
> (1) The existence of facts in respect of which there is a reasonable expectation of privacy; and
>
> (2) publicity given to those private facts that would be considered highly offensive to an objective reasonable person.

They also said there was a defence enabling publication to be justified by legitimate public concern in the information.[584]

6.23 Tipping J put the matter slightly differently. He would have set the level of offensiveness as "substantial" rather than "high", and was inclined to believe that offensiveness merged with the first requirement.[585] In other words, he took the view that offensiveness is simply one of the criteria by which one judges whether there is a reasonable expectation of privacy. He agreed that there was a defence of legitimate public concern.

Reasonable expectation of privacy

6.24 This formulation is found not just in New Zealand. It appears in all the English authorities. It is apparent from the elements stated in *Hosking* that the phrase is a fuller rendition of "private facts". As Gleeson CJ pointed out in the *Lenah Meats* case, there is no bright line between what is public and what is private.[586] To determine whether there is a reasonable expectation of privacy in relation to facts requires an exercise of judgement. Some cases are clear: serious health matters, domestic relationships, sexual activity and proclivity, and probably also financial information. Other cases are more marginal and there might well be a lack of consensus as to whether they raise a reasonable expectation of privacy. Already in New Zealand the question has been raised of whether a man had a reasonable expectation of privacy in relation to a confession of murder made to the Police.[587] The High Court and Court of Appeal thought so, but the Supreme Court did not. One may be concerned that the test is too uncertain and too subjective. Can we confidently proclaim that there is a standard of reasonable expectation which is common to all people in New Zealand irrespective of age, culture and experiences? The law is used to fictional standards: the reasonable person of the law of negligence, for example. But it is not quite the same, in that in negligence there are in many cases established standards of conduct against which the defendant's conduct may be measured. That is not usually the case with privacy.

6.25 The question is whether, if we are to have a privacy tort, it will ever be possible to provide a much sharper and more precise test than this. No doubt when enough cases have been identified their facts, and the precedents they establish,

583 *Hosking v Runting* [2005] 1 NZLR 1, para 117.

584 *Hosking v Runting* [2005] 1 NZLR 1, para 129.

585 *Hosking v Runting* [2005] 1 NZLR 1, para 256.

586 *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199, para 42.

587 *Rogers v Television New Zealand* [2008] 2 NZLR 78.

will provide a little more clarity. But this will take time. If the tort was defined by statute, the statute would be able to provide examples, or considerations to be taken into account, in deciding whether a reasonable expectation exists. The New South Wales Law Reform Commission has suggested a list of such considerations.[588] Adapted for the purpose of the New Zealand privacy tort, which is currently confined to publicity given to private facts, it includes the following:

- the relationship, whether domestic or other, between the parties;
- the effect of the publication on the health and welfare, or the social, business or financial position, of the plaintiff or his or her family or relatives;
- the place where, and the occasion on which, the facts took place;
- the age of the parties;
- any office or position held by the plaintiff or defendant;
- the purpose for which the information or other material was obtained or was intended to be used;
- the manner in which the information was obtained;
- the conduct of the plaintiff, including the extent to which the plaintiff has sought publicity in the past; and
- the extent to which the information has already been published.

Some questions about reasonable expectation

6.26 The test of reasonable expectation requires that the information be of such a character that there is a reasonable expectation that it will not be published. Indeed, in this context the word "privacy" appears to mean little more than "non-publication". The test raises some complicated issues.

Public place

6.27 It now seems to be generally accepted that the fact that something occurs in a public place does not necessarily mean there can be no expectation of privacy in relation to it. Generally speaking, if I venture into public and do something there which can be seen by anyone present, I can scarcely describe the activity as a private one. But there may be situations where something happens to me which I could not reasonably have anticipated or guarded against, and which is so humiliating or distressing that I can reasonably expect that it will not be published to the world.[589] The concern is not so much that I am observed, but that a record is made and published. Well-known examples are those of the woman who is photographed when her dress is blown up by the wind in the street;[590] where close-up pictures are taken of an accident victim who is badly injured and greatly distressed;[591] or where footage is obtained of a man with a knife who has attempted to commit suicide by cutting his wrists in the street.[592]

588 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP 1, Sydney, 2007) para 7.11.

589 See Nicole Moreham "Privacy in Public Places" (2006) 65 CLJ 606.

590 See *Daily Times Democrat v Graham* (1964) 276 Ala 380, where a woman's dress was blown up by an air vent in a fun park.

591 Example given by Young J in *Bathurst City Council v Saban* (1985) 2 NSWLR 704, 707-708.

592 *Peck v UK* [2003] EMLR 287 (ECHR).

6.28 In some cases, too, technological means may be used to defeat people's reasonable expectations of privacy: for example, a long-range microphone could be used to record a conversation taking place in a public place without the knowledge of the participants in the conversation. Even though the conversation is taking place in public, those taking part would not normally expect to be heard and recorded by people located some distance away. Where such means are used to obtain private facts about a person, there may be a legitimate concern to prevent publication of those facts. We return to questions of surveillance and other intrusive means of gathering information in Part 3 of this issues paper.

6.29 In the Naomi Campbell case, one of the constituents of Campbell's privacy action was that she had been photographed in the street having just emerged from a drug rehabilitation clinic.[593] In the New Zealand case of *Andrews*,[594] a television programme captured an intimate conversation between a husband and wife who had just been badly injured in a car crash. The Judge found that even though they were filmed in a public place by the side of the motorway, they could reasonably expect that the conversation would not be published (although he found on other grounds that their privacy action failed).

6.30 The courts of Europe and England appear to be taking this to a considerable distance. There are cases in those jurisdictions holding that photographs of a celebrity,[595] or a celebrity's child,[596] taken in the street going about their normal business can be a breach of privacy. It may be that in those cases there was an element of persistence amounting to harassment, but the conduct captured on camera was in no way embarrassing. In the light of the facts of the *Hosking* case itself, it is unlikely that a New Zealand court would reach the same conclusion. Yet the whole question of privacy in a public place is one on which views differ sharply and on which the current law is less clear than one would like.

6.31 The Broadcasting Standards Authority has for its own purposes formulated this test:[597]

> In general an individual's interest in solitude or seclusion does not prohibit recording, filming or photographing that individual in a public place (the public place exemption). The public place exemption does not apply when the individual whose privacy has allegedly been infringed was particularly vulnerable, and where the disclosure is highly offensive to an objective reasonable person.

6.32 Some might think that "particularly vulnerable" puts the matter too high. Nicole Moreham prefers this:[598]

> People should be presumed to have a reasonable expectation of privacy if they are involuntarily experiencing an intimate or traumatic experience in public, they are in a place in which they reasonably believe themselves to be imperceptible to others, or the defendant has used technological devices to penetrate his or her clothes or other self-protection barriers.

593 *Campbell v MGN Ltd* [2004] 2 AC 457.

594 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576.

595 *Von Hannover v Germany* [2004] EMLR 379.

596 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446.

597 Broadcasting Standards Authority "Privacy Principles", principle (iii).

598 Nicole Moreham "Privacy in Public Places" (2006) 65 CLJ 606, 635.

Public figures and their families

6.33 Some people are frequently in the public eye. They include politicians, people prominent in business, television personalities, sports stars, fashion models and entertainers such as actors and singers. Such people must no doubt expect more publicity than the rest of us. Some, particularly politicians, are people who influence our lives and whom we vote into office; as such we may feel we have a right to know a lot about them. Some celebrities actively court publicity, and even employ agents to see that they get it in ample measure. Yet even the rich and famous have a right to a degree of privacy. Not all of their activities are of concern to the public, as Gault P and Blanchard J recognised in *Hosking v Runting*.[599]

6.34 It is a more controversial topic in what circumstances the families, especially the children, of public figures have reduced expectations of privacy. Gault P and Blanchard J in *Hosking* recognised that:[600]

> It is a matter of human nature that interest in the lives of public figures also extends to interest in the lives of their families. In such cases the reasonable expectations of privacy in relation to at least some facts of the family's private lives may be diminished.

Their Honours did recognise, however, that the vulnerability of children must be accorded real weight.

6.35 More recently, in England, the Court of Appeal has taken a line more protective of the children of celebrities. In the *Murray* case,[601] the eighteen-month-old son of author JK Rowling was photographed in the street. The pictures were for the *Sunday Express* magazine. The Court of Appeal held that his parents were entitled to proceed with a privacy action on his behalf. Clarke MR put the matter in this way: "If a child of parents who are not in the public eye could reasonably expect not to have photographs of him published in the media, so too should the child of a famous parent."[602] He cited observations from a recent book on privacy:[603]

> The acid test to be applied by newspapers in writing about the children of public figures who are not famous in their own right … is whether a newspaper would write such a story if it was about an ordinary person.

That is not easily reconcilable with *Hosking*. Indeed, the English Court of Appeal disagreed with the *Hosking* decision.[604] The reasonable expectation of the children of celebrities is thus a matter on which there is a difference of opinion. So far the New Zealand courts are more liberal to the media.

599 *Hosking v Runting* [2005] 1 NZLR 1, para 121.

600 *Hosking v Runting* [2005] 1 NZLR 1, para 124.

601 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446.

602 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, para 46.

603 Michael Tugendhat and Iain Christie *The Law of Privacy and the Media* (Oxford University Press, Oxford, 2006) para 13.128, quoted in *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, para 46.

604 *Hosking v Runting* [2005] 1 NZLR 1, para 51.

Children and young people

6.36 In addition to the question raised above about whether the children of celebrities have a reduced expectation of privacy, there is a wider question of whether children and young people should be considered to have a greater expectation of privacy than adults. The particular vulnerability of children could also be taken into account in other ways, such as when the offensiveness of publication is considered. The Convention on the Rights of the Child, to which New Zealand is a signatory, requires states to protect children's privacy (article 16), and to make "the best interests of the child" a primary consideration in all actions concerning children (article 3(1)). At the same time, there is a public interest in reporting on matters concerning children, and this means that the media will often need to interview and photograph children.[605]

6.37 The Broadcasting Standards Authority has a provision about children. It reads:[606]

> Children's vulnerability must be a prime concern to broadcasters, even when informed consent has been obtained. Where a broadcast breaches a child's privacy, broadcasters shall satisfy themselves that the broadcast is in the child's best interests, regardless of whether consent has been obtained.

6.38 In a recent case concerning restrictions on publication under the Guardianship Act 1968, Baragwanath J observed that the importance of the right to privacy in that case:[607]

> derives from the weight placed by law and society on the need for protection of the human dignity of those who are not of an age to exercise personal autonomy and to handle the asperities of adult life.

Those "asperities", he continued, include "the need for some sacrifice of personal privacy" to accommodate freedom of expression:[608]

> But our legal history shows that children's privacy rights are not to be compared with those of adults. While not stated expressly in the Bill of Rights, their outstanding importance is recognised by common law and statute alike.

6.39 In *Hosking v Runting*, Gault P and Blanchard J considered that "the vulnerability of children must be accorded real weight and their private lives will seldom be of concern to the public", but that the basic elements of the tort provided "adequate flexibility to accommodate the special vulnerability of children".[609]

---

605 For further discussion of children's privacy and the media see Michael des Tombe "'Get that Camera out of my Face!': A Look at Children, Privacy and the Broadcasting Standards" (2000) 31 VUWLR 577; Peter Highton "Protection of Children's Privacy in the Media" (2006) 5 New Zealand Family Law Journal 147; Rosemary Tobin "Children in the Media: Privacy Implications for New Zealand" (paper for the Annual Conference, Centre for Media and Communications Law, University of Melbourne, 20-21 November 2008).

606 Broadcasting Standards Authority "Privacy Principles", principle (vii).

607 *Television New Zealand Ltd v Solicitor-General of New Zealand* [2008] NZCA 519, para 85 Baragwanath J.

608 *Television New Zealand Ltd v Solicitor-General of New Zealand* [2008] NZCA 519, para 85 Baragwanath J.

609 *Hosking v Runting* [2005] 1 NZLR 1, paras 145, 147.

Prior publication

6.40 Generally, one would think that if something has already been published it is no longer private. Indeed, in *Hosking v Runting* Gault P and Blanchard J said that "private facts are those that may be known to some people but not to the world at large."[610] But it may be that some material is of such sensitivity that the subject of it can reasonably expect that even if it has been widely published previously it will nevertheless not be published again. In *Hello! Ltd v Douglas*,[611] the English Court of Appeal thought that this was particularly so of photographs. Even if an intrusive and embarrassing photograph, perhaps of a person sunbathing topless, has been published widely, it can still be said to be reasonable to expect that it will not be published again. Likewise, a conviction which appeared in the media at the time may now be so far in the past that it would be unreasonable to revive it. So, the answer to this question is not straightforward. It is fact- and context-specific. It has been said in this country that "it is appropriate to look realistically at the nature, scale and timing of previous publications."[612]

6.41 The Broadcasting Standards Authority has developed this principle:[613]

> It is inconsistent with an individual's privacy to allow the public disclosure of some kinds of public facts. The "public" facts contemplated concern events (such as criminal behaviour) which have, in effect, become private again, for example through the passage of time. Nevertheless, the public disclosure of public facts will have to be highly offensive to an objective reasonable person.

6.42 A particular issue that is arising with increasing frequency concerns publication of material on the internet and subsequent republication in the "mainstream" media. It has become very common for journalists to turn to social networking sites either to find interesting stories, or to find background information about people who have already become of interest to the media.[614] The material they find there is usually generated by the person of interest himself or herself, although it will sometimes also be material written by others. Often the social networking pages in question are publicly accessible without using a password, but they have been written for an audience of friends and acquaintances and not for the world at large. Publication in the print or broadcast media (including websites associated with those media) can bring them to a much wider audience. This certainly raises ethical questions for journalists, especially as many of the comments from social networking sites quoted by the media are from children and young people who may not be fully aware of the potential for their comments to be used in the media.[615] The question for the development of the tort

610 [2005] 1 NZLR 1, para 119.

611 *Hello! Ltd v Douglas* [2006] QB 125, para 105.

612 *TV3 Network Services v Broadcasting Standards Authority* [1995] 2 NZLR 720, 731 Eichelbaum CJ.

613 Broadcasting Standards Authority "Privacy Principles", principle (ii).

614 Jason Spencer "Found in (My)Space" (October/November 2007) *American Journalism Review* www.ajr.org (accessed 20 January 2009). For a New Zealand example see Elizabeth Binning "Police Probe Murder Claims on Bebo" (11 September 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 1 October 2007).

615 The ethics of using such material was discussed on Radio New Zealand National "Mediawatch" programme, 23 September 2007.

is whether prior publication of personal information on a social networking site, video-sharing site or blog should result in a reduced expectation of privacy with respect to that information.[616]

When does the expectation arise?

6.43 This matter is related to the last. There have been differing views as to the moment when the expectation of privacy arises. Is it the time of the occurrence of the facts in question or the time when they are, or are about to be, published? In *Rogers*,[617] a man had allegedly confessed to a murder in a police interview. The confession was subsequently held to be inadmissible in his trial. He was acquitted. Some time later a TV channel proposed to broadcast the video of the confession. A majority of the Court of Appeal[618] held that, while Rogers might have had no expectation of privacy at the time he made the confession (he made it knowing it might be used in evidence against him in open court), such an expectation had developed by the time of the projected publication. The holding that the confession was inadmissible gave rise to an expectation that it would not be made public. The majority of the Court of Appeal held that, since publicity was the essence of the tort, the time of the projected publication was the relevant one. However, the Supreme Court[619] held differently. They found that the nature of the confession was such that Rogers could never reasonably have assumed it would be private. The matter of timing was not much discussed in the judgments. Tipping J said that he did not consider that Rogers had any reasonable expectation of privacy in the confession or the video tape which recorded it, "whatever date is taken for that assessment."[620] McGrath J likewise thought there was no reasonable expectation of privacy at any time.[621] This question has thus not been answered definitively by *Rogers*. There is other authority, however, to the effect that matters once public can become private by lapse of time. Previous convictions, as we have already discussed, might be an example,[622] a conclusion to some extent supported by the Criminal Records (Clean Slate) Act 2004. However, the matter awaits clarification.

Plaintiff culpability

6.44 There is also a lack of clarity as to whether the conduct of the plaintiff can disentitle him or her to succeed in an action of invasion of privacy. In *Andrews,* while Allan J apparently believed there was merit in this contention, it was not necessary to explore it in detail. In that case it was argued that the plaintiffs were

616 A complaint to the Press Council that quotations in a newspaper from the Bebo page of a 14-year-old boy breached the boy's privacy was successful: *English v Southland Times* (February 2008) Press Council Case No 2019. A woman in the United Kingdom is suing for defamation and breach of privacy over newspaper reports based on information on her daughter's Bebo page: Robert Verkaik "Bebo Booze-Up Story Sparks Six Lawsuits" (11 July 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 14 July 2008).

617 *Rogers v Television New Zealand* [2008] 2 NZLR 78.

618 [2007] 1 NZLR 156.

619 *Rogers v Television New Zealand* [2008] 2 NZLR 78.

620 *Rogers v Television New Zealand* [2008] 2 NZLR 78, para 68.

621 *Rogers v Television New Zealand* [2008] 2 NZLR 78, para 105.

622 See, eg, *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716. See also Broadcasting Standards Authority "Privacy Principles", principle (ii); Rogers *v Television New Zealand* [2008] 2 NZLR 78, para 26 Elias CJ.

disentitled from succeeding in their privacy action because they had been driving while intoxicated.[623] The argument presented was that a plaintiff's own conduct may be such that it reduces or eliminates any expectation of privacy that the person might otherwise have had.

6.45 There is probably no equivalent of a "clean hands" rule in this tort. That doctrine is of equitable origin and it would seem unorthodox to apply it in the present context. The difficulty with the argument is that it involves at least four different strands. It is this that causes the uncertainty about it.

6.46 First, if the conduct of the plaintiff which is to be published was contrary to the public interest, the defendant may be entitled to publish it under the public concern defence.

6.47 Secondly, "there is no confidence [or, one might add, privacy] in iniquity."[624] Some of the early English courts have taken this some distance, and held that immoral conduct such as adultery, or a liaison with a prostitute, do not merit protection under our privacy laws. In *A v B plc*,[625] Lord Woolf said that a one-night stand was not a relationship which deserved privacy protection in the way that a long-term relationship such as marriage did. Today, however, that attitude seems to be softening. Judges are concluding that they are not guardians of the public morals in these matters and should not impose their own moral opinions on others. Thus, an injunction was recently granted to a man to prevent disclosure of an adulterous relationship on the ground that it would be an invasion of his privacy,[626] and another was awarded damages for the publication of details of sadomasochistic activity in which he participated with women who were paid for their involvement.[627]

6.48 Thirdly, there is some early authority that a celebrity who courts favourable media publicity cannot complain if the media show up their less attractive side, and in the course of doing so reveal conduct that might otherwise be regarded as private.[628] This is an argument based on hypocrisy. Once again there have been intimations, at least in the English courts, that this argument carries less weight than it once did.[629] Yet one would have thought that, at least in the more extreme cases, there would be some merit in the argument. Surely a celebrity cannot be allowed entirely to dictate how he or she is portrayed to the world.

6.49 Fourthly, one thing is clear. If a person misleads the public by telling untruths about him or herself, the media must be allowed to refute them, even if in so doing they disclose otherwise private information. That was the basis of the holding in *Campbell*[630] that the media were allowed to go to a reasonable extent in demonstrating that Campbell had been untruthful when she said she did not

623 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576, paras 42-47.

624 *Gartside v Outram* (1857) 26 LJ Ch 113, 114 Wood VC.

625 [2003] QB 195.

626 *CC v AB* [2007] EMLR 312.

627 *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), para 128. Eady J said that where the law is not breached "the private conduct of adults is essentially no-one else's business."

628 *Woodward v Hutchins* [1977] 1 WLR 760; *Lennon v News Group Newspapers* [1978] FSR 573.

629 *McKennitt v Ash* [2008] QB 73, paras 33–36.

630 *Campbell v MGN Ltd* [2004] 2 AC 457.

have a drug habit. However, there is always a question in cases like this of how much private detail it is necessary to go into to refute the untruths. A newspaper needs to be allowed to give enough detail to make its case, but there can be disagreement as to exactly where the line is to be drawn. *Campbell* itself was just such a case. There the House of Lords divided three to two on how much detail it was appropriate to publish.

6.50 So the "plaintiff culpability" argument dissolves into a number of strands. In *Andrews*, Allan J admitted its validity, but did not elaborate on its extent. He said:[631]

> I accept however that an expectation of privacy otherwise reasonable may in certain circumstances be lost by reason of culpability on the part of the plaintiff. It is to be observed that the same consideration might well arise in a given case in the course of an assessment of whether the publication of private facts is highly offensive and further in relation to the assessment of a defence of legitimate public concern.

But he thought it was "difficult, and indeed undesirable, to lay down any general principle governing the extent to which personal culpability might impinge upon reasonable expectations of privacy."

6.51 Once again, if one were to contemplate a statutory tort of privacy this may be a matter which could be addressed.

Highly offensive

6.52 Because of the propensity of a tort of privacy to collide with freedom of expression, the Court of Appeal in *Hosking* was concerned to keep it within tight confinement.[632] The judgment of Gault P and Blanchard J does this by prescribing not only that there must be a reasonable expectation of privacy, but also that the publication of the facts must be highly offensive to an objective reasonable person. This replicates the test adopted in the United States cases, and also the test used since its inception by the Broadcasting Standards Authority.

6.53 Under the *Hosking* formulation both elements must be proved. In *Andrews*,[633] the cumulative nature of the tests was decisive. Allan J decided that while Mr and Mrs Andrews did have an expectation that their conversation at the roadside would not be broadcast, it was nonetheless not highly offensive to do so. The content of what was said between the parties was not particularly embarrassing or sensitive.

6.54 In other words, what we have in New Zealand is a two-step test. First, is there a reasonable expectation of privacy in this matter? Secondly, is the transgression in this case sufficiently serious to warrant the intervention of the law?

631 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576, para 47. See also Lisa Tat "Plaintiff Culpability and the New Zealand Tort of Invasion of Privacy" (2008) 39 VUWLR 365.

632 *Hosking v Runting* [2005] 1 NZLR 1, para 130.

633 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576.

Should it be a separate test?

6.55 There is, however, a lack of unanimity as to whether the highly offensive test should be a separate requirement. In *Hosking* Tipping J, differing from Gault P and Blanchard J, was inclined to think it was merely a factor to take into account in deciding whether in a particular case there existed a reasonable expectation of privacy.[634] This is very similar to the view taken by Gleeson CJ in the *Lenah* case:[635]

> Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.

The English courts do not regard the highly offensive test as a separate requirement. Lord Hope, after citing Gleeson's CJ dictum, said:[636]

> The test which Gleeson CJ has identified is useful in cases where there is room for doubt, especially where the information relates to an activity or course of conduct such as the slaughtering methods that were an issue in that case. But it is important not to lose sight of the remarks that preceded it. The test is not needed where the information can be easily identified as private.

6.56 So, according to this approach, the highly offensive test is applicable only where the decision as to whether there is a reasonable expectation of privacy is a marginal one. There is some support for the view that the requirement should not be a separate one in New Zealand. Nicole Moreham expresses that view.[637] As noted earlier in this chapter, she believes that, since privacy is a dignitary tort, it is actionable without proof of damage, so any interference is prima facie actionable. The highly offensive test postulates that injury in the form of offence is necessary. In *Rogers*, Elias CJ signalled that she also believes that the question is open for reconsideration.[638]

6.57 Yet one could argue that a separate requirement of "highly offensive" does perform a proper function. The formulation of Gault P and Blanchard J in *Hosking* makes it clear that it is the *publication* of the information to which the requirement of "highly offensive" attaches.[639] While there may be some information which is so sensitive and private that *any* publication of it would be highly offensive, this may not always be the case. Thus, one could imagine a case where the broadcast of a brief news item showing the victim of a motor

634 *Hosking v Runting* [2005] 1 NZLR 1, para 256.

635 *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199, para 42.

636 *Campbell v MGN Ltd* [2004] 2 AC 457, para 94. See also *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, paras 25–30.

637 NA Moreham "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation: Essays in Honour of John Burrows QC* (LexisNexis NZ, Wellington, 2008) 231.

638 *Rogers v Television New Zealand* [2008] 2 NZLR 78, para 25.

639 Emphasised by Gault P and Blanchard J in *Hosking v Runting* [2005] 1 NZLR 1, para 127.

crash would be acceptable, but where repeated use of the footage, or perhaps a close-up of the injury in a documentary, would not be. The case would be even clearer if the items showing the plaintiff's distress were to be shown in a comedy programme, or put on the internet. In other words there are cases where the impact of the publication of certain facts varies depending on the context in which that publication takes place. The requirement of "highly offensive" might therefore have true independent force.

6.58 Furthermore, there can surely be no jurisdiction which would regard even the most trivial infringements of privacy as being actionable. In *McKennitt v Ash* it was noted that, before the privacy article of the European Convention is engaged, there must have been an interference with private life "of some seriousness."[640] So even in that jurisdiction a threshold must be reached. In New Zealand, Gault P and Blanchard J have decided to pitch that level of seriousness high. It must cause a high level of offence. The Broadcasting Standards Authority likewise regards it as a requirement, and has done so for 18 years. It would be unfortunate if the common law tort and the standards applied by the BSA diverged in a way which could be confusing to broadcasters. New Zealand's commitment to freedom of expression under the Bill of Rights Act might argue for a balance between privacy and freedom of expression which gives significant weight to the latter.

6.59 Whether the requirement of "highly offensive" is necessary needs authoritative determination. We note that the Australian Law Reform Commission specifies it as a requirement of the statutory cause of action which it recommends.[641]

Offensive to whom?

6.60 It appears to be settled that, assuming the "highly offensive" test is applicable, it is not just the reasonable reader who must be offended. It is an objective reasonable person in the shoes of the plaintiff. The question, in other words, is "how would I feel if this had been published about me?"[642] Like "reasonable expectation of privacy", this requires a delicate exercise of judgement. It is probably true that even people of similar backgrounds and habits might occasionally disagree on such a question. It is much more difficult if the plaintiff in whose shoes one is temporarily standing is a person of a different culture, or a markedly different age, or placed in decidedly different circumstances. Such a case was *Attorney-General v Brown* where Brown, a convicted paedophile, had been released into the community. The Police issued flyers picturing and naming him, and locating the area where he lived. Brown succeeded in his privacy action. In relation to the "highly offensive" requirement the Judge noted:[643]

640 [2008] QB 73, para 12, citing *M v Secretary of State for Work and Pensions* [2006] 2 AC 91, para 83. Compare *Lord Browne of Madingley v Associated Newspapers Ltd* [2008] QB 103, para 33, where it was said that apparent triviality does not necessarily rule out a claim. But here there was clearly a confidential relationship between the parties.

641 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) R74-2.

642 This was stated as early as *P v D* [2000] 2 NZLR 591, para 39 Nicholson J. The test was approved in *Campbell v MGN Ltd* [2004] 2 AC 457, para 100 Lord Hope. See also *Brown v Attorney-General* [2006] DCR 630.

643 [2006] DCR 630, para 81 Judge Spear.

> The test of course is not for the objective reasonable paedophile but of a reasonable person in the shoes of the person that the publication is about … I am just able to find that an objective reasonable person, standing in the shoes of the plaintiff, should be highly offended by the publication of that information about the plaintiff. That person should also find the resultant vilification to be highly alarming and offensive.

6.61 Nor can it have been much easier in *Rogers*, where the plaintiff was a man who had confessed to murder.[644] In circumstances like these, the test is by no means easy of application. It is not conducive to certainty or predictability. It is probably more dependent on subjective and instinctive judgment than even "reasonable expectation of privacy."

Public concern

6.62 Freedom of expression and privacy are both expressly protected in the European Convention on Human Rights. Each case involves a balancing between them. The English courts follow the Convention closely. In *Re S*, Lord Steyn thus explained the reasoning process to be followed:[645]

> First, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justifications for interfering with or restricting each right must be taken into account. Finally the proportionality test must be applied to each. For convenience I will call this the ultimate balancing test.

6.63 In New Zealand it is a little different. Freedom of expression is an express right in the Bill of Rights Act, while privacy is not. *Hosking v Runting* establishes that a tort of privacy exists, presumably as a justified limitation on freedom of expression within section 5 of the Bill of Rights Act, but freedom of expression reasserts itself in the form of a defence of legitimate public concern. The onus is on the defendant to establish that defence. The expression used in the judgment is *legitimate public concern*, not *public interest*, a phrase well known in other areas. The expression emphasises two things. First, more is required than something which merely interests or titillates the public: it must be something which is of genuine importance to them. Secondly, what is required is more than something that is simply newsworthy, otherwise the media themselves would be arbiters of what the public interest requires.[646]

6.64 The ultimate decision of what is of public concern lies with the court, if the matter proceeds that far. The defence raises the following questions. Once again, the main concern is its indeterminacy and consequent uncertainty.

6.65 First, the term *public concern,* like the more familiar *public interest*, is one that does not admit of ready definition. *Public interest* appears in many places in our law – there are over 500 references to it in our statute book, and it is well known in defamation and breach of confidence. It has been described as "a yard-stick

644 *Rogers v Television New Zealand* [2008] 2 NZLR 78.

645 *Re S (a Child)* [2005] 1 AC 593, para 17.

646 See discussion in *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), paras 135 and 138.

of indeterminate length."[647] It can vary with time and place. One of the most useful attempts to give it some content is by the Broadcasting Standards Authority. They have said that includes:[648]

- criminal matters, including exposing or detecting crime
- issues of public health or safety
- matters of politics, government, or public administration
- matters relating to the conduct of organisations which impact on the public
- exposing misleading claims made by individuals or organisations
- exposing serious anti-social and harmful conduct.

6.66 This catalogue received the approval of Harrison J in the High Court in *Canwest TV Works Ltd v XY*.[649] The decisions of the courts in breach of confidence cases show that the following matters have been deemed to be of sufficient public interest to override an obligation of confidence: police corruption; the dangerous effects of the doctrine of a fringe religion; the fact that an alcohol breath-testing device was seriously inaccurate; malpractice in a national security service; airline safety; fraud on the revenue; and the business case for setting up a new bank.[650] Having said that, however, the category is open-ended, and at the margins can involve a judgement on which individuals may disagree.

6.67 Secondly, although, for the reasons given, the exercise in New Zealand is rather different from that undertaken in England, proportionality is still relevant in this country. The greater the infringement of privacy, the greater will the public concern need to be to override it, and vice versa.[651] The required balancing exercise is ultimately one of *impression*.

6.68 Thirdly, the decision will not always be straightforward. Indeed, in a particular case there may be competing public interests which press in different directions. The exercise often involves more than balancing the private interest of the individual against a single public interest: public interests themselves can compete. This was the case in *Brown v Attorney-General*,[652] the case of the convicted paedophile who had been released from prison. Brown claimed invasion of his privacy by publication of the flyers. Public interest pushed in two different directions. On the one hand, one might have thought there was a clear advantage to parents to know of the man's presence in the area. Forewarned is forearmed. On the other hand, evidence was produced to the court that public shaming of this kind can often make matters worse and increase the risk of offending by preventing the person's proper integration into society. It might also create a real risk (here realised) of vigilante action by members of the public. The court, having weighed up all the arguments in a difficult balancing exercise, concluded that the public interest lay in favour of non-publication. Brown won the case and was awarded damages.

---

647 *Attorney-General v Car Haulaways (NZ) Ltd* [1974] 2 NZLR 331, 335 Haslam J.

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

649 [2008] NZAR 1.

650 See John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, Auckland, 2005) 223–225.

651 *Hosking v Runting* [2005] 1 NZLR, para 134 Gault P and Blanchard J; para 257 Tipping J.

652 [2006] DCR 630.

6.69 Fourthly, the mere fact that the general subject of an article or broadcast is of public concern does not of itself justify the inclusion of intimate private detail. The details have to be related to the matter of public concern and must have value in illustrating the points made. The reference to them must not be simply gratuitous. So in the *Andrews* case,[653] it might be argued that the matter of public concern, the work of the Fire Service, could have been demonstrated without playing the Andrews' conversation. Here again, different minds may differ on how much detail is acceptable. But one must take into account the reality of the modern media and its audience. People do not read newspapers, and do not watch television programmes, unless they are interesting. Illustrative detail makes them more interesting. So in the *Rogers* case in the Court of Appeal, William Young P said:[654]

> I agree that the underlying issues can be debated without the videotape being shown on national television, but experience shows that arguments are usually more easily understood when they are contextualised. An esoteric argument … becomes far more accessible to the public if the implications can be assessed by reference to the concrete facts of a particular case.

In *Andrews*, Allan J said: "In assessing an asserted defence of legitimate public concern the court will ordinarily permit a degree of journalistic latitude so as to avoid robbing a story of its attendant detail which adds colour and conviction."[655] In other words, unless the item appeals to the public, it may fail to achieve the benefit of informing the public about the matter of public concern. Having said that, the limits are not at all easy to draw.

6.70 Fifthly, once the exercise has been completed and the court has determined that the public concern either does or does not outweigh the privacy interests of a plaintiff, the question is how readily an appeal court should overturn that determination. In England, appeal courts are not ready to substitute their own judgment for that of the first instance Judge. The balancing that he or she has performed is treated in the same way as the exercise of the discretion.[656] It is not clear whether the New Zealand courts will take the same line where public concern is treated as a defence to a claim. However, in the *Rogers* case in the Court of Appeal, Panckhurst and O'Regan JJ did say that the matter was one of evaluation on which there should be appellate restraint.[657] In that case, though, the court did disagree with the conclusion of the High Court.

6.71 Sixthly, we note that the Canadian provinces require only *reasonable grounds for belief* that the matter published was of public interest, rather than making the public interest an absolute requirement. That is the case also with a recent amendment to the Data Protection Act 1998 (UK) which provides that it is a defence to the offence of unlawfully obtaining personal data that the defendant acted with a view to publication of journalistic, literary or artistic material and "in the reasonable belief that in the particular circumstances the obtaining,

653 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576.

654 *Rogers v Television New Zealand* [2007] 1 NZLR 156 (CA), para 128.

655 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576, para 82.

656 See *Campbell v MGN Ltd* [2004] 2 AC 457, paras 87, 101 and 158; *McKennitt v Ash* [2008] QB 73, para 45.

657 *Rogers v Television New Zealand* [2007] 1 NZLR 156 (CA), para 90.

disclosing or procuring was justified as being in the public interest."[658] It is also of interest that in the *Mosley* case, Eady J foreshadowed the possibility of a "responsible journalism" test which might afford the media a defence if they had taken all reasonable steps to check their sources, but still formed a mistaken impression that the matter was of public concern.[659] However, we believe that while a requirement of reasonable belief may be appropriate in the criminal law, it is less satisfactory in tort. In other areas, such as breach of confidence and the defence of honest opinion in defamation, it is the *existence* of public interest that matters and not reasonable belief of it. The "responsible journalism" test had its genesis in the United Kingdom in the defence of privilege in defamation, and it is too early to assess how far it will be applied even in defamation cases in New Zealand. The maintenance of the present objective "legitimate public concern" defence would seem more in line with principle.

6.72 Seventhly, another matter deserves mention. The "public concern" test is particularly appropriate where there has been wide publicity through the media. If, however, it can in some circumstances amount to a tort to disclose private information to a few persons or even to only one (which is currently not certain), the "public concern" formulation may not always seem quite so appropriate. What, for example, of a case where an employee discloses to an employer, in the interests of the business, disgraceful private conduct of another employee? Such information may be of great concern to the employer, but of little or none to the public. However, where facts of this kind arise, should they ever do so, the more appropriate defence is likely to be privilege, rather than the public concern defence.

6.73 We conclude that the "legitimate public concern" defence adds a further dimension of uncertainty. The statutes of the Canadian provinces, in addition to a general public interest requirement, also specify a few particular instances of matters of public interest: for example, that of "a public officer engaged in an investigation in the course and in the scope of his duty."[660] If the matter were ever to be codified in New Zealand it would be possible to provide further illustrations, or indeed a list of the kind provided by the Broadcasting Standards Authority, but such a list could never be exhaustive.

Remedies

Damages

6.74 The *Hosking* court made it clear that damages are to be the main remedy for breach of privacy. Yet we demonstrated earlier in the chapter that injury to dignity is an intangible which it is not possible to measure with precision. The lack of any real jurisprudence on compensation for loss of dignity is a difficulty in this area. On the one hand, one does not want to encourage gold-digging actions, and one would at the very least expect a sensible

658 Criminal Justice and Immigration Act 2008 (UK), s 78, amending Data Protection Act 1998 (UK), s 55(2). This amendment has not yet come into force.

659 *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), paras 140-142.

660 Privacy Act 1978 RSS c P-24, s 4 (Saskatchewan); Privacy Act 1990 RSNL c P-22, s 5 (Newfoundland and Labrador); Privacy Act 1996 RSBC c 373, s 2 (British Columbia); Privacy Act CCSM s P125, s 5 (Manitoba).

relativity with ACC compensation for physical injury. On the other hand, it needs to be borne in mind that if damages are trifling few plaintiffs would be prepared to go to the trouble, embarrassment and cost of bringing their private concerns before that very public body, a court. The fewer the cases, the less the incentive to respect privacy.

6.75 It may some time have to be determined whether exemplary damages are appropriate in this area of the law. We are inclined to think not. They are a controversial remedy in other areas of tort law. Some commentators have called for their abolition, on the grounds that it is not the function of civil action to punish the defendant. However, whatever may happen to exemplary damages in other branches of the law, we believe that their incidence should not be expanded, and that they should have no place in the privacy tort. Eady J took the same view in the *Mosley* case, although one of his reasons was that in England invasion of privacy is not regarded as a tort.[661]

6.76 Given the difficulty of assessing damages in this area of the law, this is perhaps a subject where statute could add clarity. It could, for example, provide that damages are not confined to distress and humiliation but that they can extend to financial and other loss. Section 88 of the Privacy Act 1993 is a precedent. Statute could also lay down a non-exhaustive list of considerations to be taken into account in assessing damages. They might include the extent of publication; the conduct of the defendant after publication; any contributory negligence by the plaintiff; the defendant's motive for publishing; the age of the plaintiff; and the extent of distress and hurt to the plaintiff. On the other hand, perhaps these matters are so obvious that they go without saying.

Injunction

6.77 It was indicated in *Hosking* that injunction will be an exceptional remedy. No doubt freedom of expression requires that an injunction, the effect of which is to suppress expression, should not be readily granted: it is a form of prior restraint. The tendency in New Zealand since the passing of the Bill of Rights Act has been to apply a strong presumption against injunctive relief in all areas of media law: defamation, contempt of court and now privacy.[662] No doubt if injunctions are easy to obtain there will be plaintiffs who will seek them to cover up their indiscretions. Even interim injunctions can sometimes remain effective for a long time. They can thus be an impediment to freedom of expression. Matters of news interest can lose their currency and value. Once the moment has passed, the item may lose context and relevance.

6.78 However, caution must be exercised before adopting a uniform approach across the board in all areas of media law. Privacy cases differ from, say, defamation cases. In defamation, if an injunction is refused and publication of the offending item goes ahead, the plaintiff's reputation can still be substantially restored by a finding that the slur on his or her reputation was unjustified, and by the award of damages which mark the seriousness of the defendant's wrongdoing. But in privacy cases damages can never quite restore

661 *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), paras 172-197.

662 See especially *TV3 Network Services Ltd v Fahey* [1999] 2 NZLR 129; Jesse Wilson "Prior Restraint of the Press" [2006] NZ Law Rev 551.

the plaintiff's lost privacy: once the cat is out of the bag it is impossible to put it back. Compensation is a poor substitute for silence. In the *Rogers* case in the Supreme Court, Elias CJ alluded to this:[663]

> The analogy with interlocutory restraint in defamation proceedings is imperfect and needs to be treated with caution. Injunctive relief may well be appropriate [in privacy cases]: whether the freedom of information considerations should prevail depends on the circumstances of the particular case and all interests properly engaged.

6.79 The Chief Justice's reference to interlocutory relief raises further special considerations. It is not an infrequent occurrence for a plaintiff getting wind that there may be a publication which will harm his or her privacy to seek an injunction a matter of hours before the publication is due to go to press or to air. If the case could involve difficult issues of, say, public concern, which will take time to prepare and argue, the court is unlikely to decline an interim injunction. In *Cream Holdings Ltd v Banerjee*, Lord Nicholls said, in relation to a section of the Human Rights Act 1998 (UK) which lays down a threshold for interlocutory injunctive relief:[664]

> The judge needs an opportunity to read and consider the evidence and submissions of both parties. Until then the judge will often not be in a position to decide whether on balance of probability the applicant will succeed in obtaining a permanent injunction at the trial. In the nature of things this will take time … What is to happen meanwhile? Confidentiality, once breached, is lost for ever. Parliament cannot have intended that, whatever the circumstances, s 12(3) [of the Human Rights Act] would preclude a judge from making a restraining order for the period needed for him to form a view on whether on balance of probability the claim would succeed at trial. That would be absurd.

6.80 It is likely in fact that injunction will be the remedy of choice for the majority of litigants. That has been the case in New Zealand since the time invasion of privacy was first mooted as a possible tort in this country. It is also the case in England. Generally speaking, plaintiffs want to stop infringements of their privacy before they happen rather than picking up the pieces afterwards.

6.81 It should also be noted that injunctions are not always against a single defendant. Injunctions against the world are rare, but not unknown;[665] there is also precedent for injunctions against persons unknown.[666] These protections are strong, but exceptional.

Other remedies

6.82 Consideration may need to be given to whether other remedies than damages and injunction should be available. One might be account of profits. If the defendant has made money out of the plaintiff's personal information, there may indeed be a case for requiring an account, so that the defendant is required to disgorge the benefit deriving from his or her unlawful conduct.

663 *Rogers v Television New Zealand* [2008] 2 NZLR 78, para 38.

664 *Cream Holdings Ltd v Banerjee* [2004] 4 All ER 617, para 18.

665 For example, *Venables and Thompson v News Group Newspapers Ltd* [2001] 1 All ER 908.

666 For example, *Brash v Doe* (16 November 2006) HC WN CIV 2006-485-2605.

Another possible remedy is an order for the delivery up of documents, to require the defendant to surrender to the plaintiff possession of damaging documents – intimate photographs, for instance.

Some gaps

6.83 So far we have examined the *Hosking* criteria, the defence of legitimate public concern and the possible remedies. There is open-endedness and difficulty of application in most of them. In respect of some, the uncertainty and consequent unpredictability at this early stage in the life of the tort is greater than one might deem desirable, particularly given privacy's contest with freedom of information. It is going to be difficult for lawyers to give confident advice.

6.84 There are also significant gaps in the tort. If it is left to the common law, it may be a long time before they are filled. Courts can only develop the law when the appropriate case arises. The common law is subject to the accidents of litigation, and it is of the nature of the privacy tort that there is unlikely to be much litigation. So, many of the questions are likely to remain unanswered for some considerable time. At least the following matters would benefit from authoritative resolution.

Falsity

6.85 Does a privacy action lie only in respect of true information or can it also lie in respect of false allegations? In *A v Hunt*, Wild J said:[667]

> A necessary aspect of the privacy tort is that the impugned, highly offensive fact be just that: a fact. That is what distinguishes the privacy tort from defamation. Falsity is an element of the tort of defamation; truth a defence to it.

This would support the proposition that false allegations are the province of defamation, not privacy. It might also suggest that one of the American variants of the tort of privacy, putting the plaintiff in a false light, has no place in New Zealand.

6.86 However, things are not quite so clear. The Broadcasting Standards Authority in its privacy jurisdiction has reached conflicting decisions about this.[668] There is also English authority for saying that in at least one situation false information may indeed be the subject of a privacy action. This is where a publication provides a lot of information about the plaintiff, some of it true, some of it partly true, some of it only doubtfully true, and some of it downright false. A plaintiff, this authority holds, should not have to go through it with a fine-tooth comb eradicating the less-than-fully-correct parts. Eady J has said:[669]

> The protection of the law would be illusory if a claimant in relation to a long and garbled story was obliged to spell out which of the revelations are accepted as true and which are said to be false or distorted.

---

667 (17 May 2006) HC WN CIV 2003–485–2553, para 58. This matter was not dealt with on appeal, where the judge's decision on other aspects was reversed: *Hunt v A* [2008] 1 NZLR 368.

668 See, on the one hand, *X v HB Media* (4 December 1997) Broadcasting Standards Authority 1997-161, and on the other *Canwest TV Works Ltd v Harris* (1 November 2005) Broadcasting Standards Authority 2005–049.

669 *McKennitt v Ash* [2006] EMLR 178, para 78.

6.87 It may perhaps even go further. Not all false information is defamatory: to say someone has a serious illness will usually not be.[670] In such a case as this, should the plaintiff's chances of success in a privacy action depend on whether the statement is true or false?[671] As Eady J has put it, "intrusion upon privacy can take place by the process of exploring or speculating on intimate subject matter irrespective of accuracy."[672] If it is concluded that false allegations are within the purview of the tort, consideration might be given to orders or recommendations for the correction of those allegations.[673]

Relationship between privacy and defamation

6.88 The relation of invasion of privacy to defamation needs to be worked through.[674] In a recent English case,[675] a deputy judge awarded damages for both defamation and privacy when the defendant placed embarrassing information about the plaintiff, some of it false, on Facebook.

Publicity

6.89 What is required by the formulation in *Hosking* is *publicity* given to facts in respect of which there is a reasonable expectation of privacy. Does this envisage widespread publication, as in the media; or is it enough that the publication is only to a few people, at least if those people are outside the circle of family and intimate friends who are likely to know the plaintiff's circumstances anyway? The test given in the American *Restatement* is that there must be "publication to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[676] In *Hosking*,[677] Gault P and Blanchard J suggested that publicity should be "widespread." Obviously publication in the media or on the internet would qualify. Yet there is limited and exceptional United States authority to the effect that sometimes lesser publication may suffice.[678] Disclosure of highly embarrassing private information to even one person – say an employer – could be hurtful and could indeed have serious consequences. The misuse of intimate health information may result in only a few unauthorised persons knowing of it, yet cause substantial embarrassment to the subject. No doubt in such a case in New Zealand the Privacy Act would often provide a remedy, but that is not the issue: the question is whether tortious damages or an injunction can be claimed. If, as we have suggested, the main interest to be protected by the new tort is human dignity, there is an argument for saying that it can be damaged irrespective of the number of people who learn of the information. Yet so to define the tort would greatly expand its potential

670 Unless it is such as to cause people to "shun and avoid" the subject.

671 See *McKennitt v Ash* [2008] QB 73 (CA), paras 79 and 80 Buxton LJ.

672 Hon David Eady "Privacy and the Media" (paper presented to Cardiff School of Journalism, 29 September 2007).

673 See for example Defamation Act 1992, s 26 (correction recommendation); Broadcasting Act 1989, s 13(1) (order directing that statement be published).

674 See *Hosking v Runting* [2005] 1 NZLR 1, paras 136–138 Gault P and Blanchard J.

675 *Firsht v Raphael* [2008] EWHC 1781 (QB). The plaintiff was awarded £15,000 for defamation, and £2000 for invasion of privacy.

676 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652D.

677 *Hosking v Runting* [2005] 1 NZLR 1, para 125 Gault P and Blanchard J.

678 See, eg, *McSurely v McClellan* (1985) 243 App DC 270.

coverage. From being a tort applying mainly to the media and other mass publishers, it would become a tort regulating any unauthorised disclosure, be in it the health sector, the employment sector, or any other.

6.90 Clarification would be helpful.

Defences

6.91 Legitimate public concern is a defence, but there has been no discussion in New Zealand as to what the other defences to the tort might be. No doubt consent is. It is a defence to all torts. It would have to be shown that the consent was a genuine consent, and was to the very kind of publication which has happened, and in respect of the same information. Action under legal authority should likewise be a defence, although it would usually be captured by "legitimate public concern". In some other jurisdictions privilege is a defence.[679] It probably should be here. If a Member of Parliament discloses information about the private life of another MP in the course of a debate in Parliament, are the media safe in reporting it? If an employee has been guilty of disgraceful conduct in private which reflects on his or her fitness to do his or her job, is another employee entitled to disclose this to the employer? Should the other employee be more disadvantaged if the information that is disclosed is true than if it is false and defamatory, in which case there clearly would be a qualified privilege? It may also be that in some situations contributory negligence might apply (if for example the plaintiff has left personal information in a place where it could readily fall into other hands) and that damages should be apportioned accordingly. However, contributory negligence is probably better regarded not as a defence, but rather as a ground for reducing damages.

6.92 In Saskatchewan it is a defence that the defendant was engaged in news gathering for a newspaper or broadcaster, and that such act, conduct or publication was reasonable in the circumstances and necessary or incidental to ordinary news gathering activities.[680] As we have seen, a recent exception to an offence in the Data Protection Act 1998 (UK) likewise contains a special media exemption. These defences are, however, mainly relevant to media intrusions (discussed in chapter 12 below) rather than publicity given to private facts. We are currently of the view that the legitimate public concern defence suffices to give the media and others adequate protection without placing the media in a special position. That conclusion is strengthened by the consideration that it becoming increasingly difficult in the new digital age to define who and what the news media are.

Plaintiffs

6.93 We discussed in our 2008 study paper the question of whether privacy can attach to bodies corporate or deceased persons.[681] These questions remain unanswered in relation to the new tort.

679 It is so in the United States, and in the statutory torts of the Canadian provinces of Manitoba, Saskatchewan, British Columbia and Newfoundland.

680 Privacy Act 1978 RSS c P-24, s 4(1)(e).

681 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 191–195.

6.94 If dignity is indeed the basis of the tort, as has been suggested, one would think that the tort is not appropriate for corporations. Dignity is a human value. It is about the inherent worth of the human being. That was the strong view of most of the Judges in *Lenah*[682] in the High Court of Australia. The weight of United States authority is in favour of that view.[683] Moreover, the Privacy Act 1993 defines "individual" as a *natural* person.[684] On this view, breach of confidence would be the appropriate course of action for a corporation, rather than invasion of privacy. However, the case is not entirely open-and-shut. A case could be made, for instance, that allowing a privacy right to a corporation protects the privacy of its constituent members. Moreover, as we have seen, there is some authority that privacy protects "autonomy". If autonomy is indeed something different from dignity, it may be appropriate to speak of the "autonomy" of a corporation. As we have also seen, courts in privacy actions are capable of awarding remedies for damage beyond humiliation and hurt feelings: financial loss, for instance. It is also of relevance that in New Zealand the Bill of Rights Act provides that it is not only human beings who can take the benefit of the rights it contains.[685] Corporations can sue for defamation, too, although only in respect of financial loss. So there are arguments to be made on both sides. The matter is unsettled.

6.95 As far as deceased persons are concerned, it is an open question whether their next of kin could bring a privacy action, and if so whether it would be their own action, or an action on behalf of the deceased's estate. As we noted in our study paper, no doubt it is proper and realistic to speak of respect for deceased persons, and even to speak of their possessing dignity. It is a criminal offence to "offer any indignity" to any dead human body or human remains.[686] Moreover, the Privacy Act 1993 acknowledges in various places a privacy interest in deceased persons.[687]

6.96 However, in the cognate tort of defamation the action dies with the deceased whether the defamatory publication took place before or after death. It may be difficult to justify any different conclusion in respect of privacy, particularly if one concludes that it protects a value which is inherently personal. If the privacy of the next of kin themselves were infringed, that would be a different matter. In the United States, the authority is not all one way. While the prevalence of US authority holds that there is no action on behalf of the deceased person,

682 *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199.

683 See David A Elder *Privacy Torts* (Thomson West, Egan (MN), 2002) para 1.4.

684 Privacy Act 1993, s 2.

685 New Zealand Bill of Rights Act 1990, s 29.

686 Crimes Act 1961, s 150.

687 "Personal information" includes information about deaths maintained by the Registrar-General pursuant to the Births, Deaths and Marriages Registration Act 1995 (s 2(1)); codes of practice concerning health information can cover health information relating to deceased persons (s 46(6)); and an agency can refuse access to personal information held by that agency if it would involve unwarranted disclosure of the affairs of a deceased individual (s 29(1)(a)).

there are a few cases holding that sometimes the next of kin may be able to sue to protect the memory of the deceased person as well as to recover for their own hurt feelings.[688] In New Zealand we must also take into account Māori tradition.[689]

Identification

6.97 The overwhelming weight of authority is in favour of the view that the plaintiff must have been identified before his or her privacy can be invaded. In *TVNZ v BA*, Miller J summed up the approach of the Broadcasting Standards Authority in applying its privacy principles:[690]

> The authority held that its first task when determining a complaint when a broadcast involves a breach of privacy, is to decide whether the complainant is identifiable from the broadcast. The complainant must be identifiable beyond immediate family and close acquaintances who may reasonably be expected to be aware of the activities for which the complainant has received publicity.

In the *Andrews* case, a case on the *Hosking* tort, Allan J likewise regarded identification as being a requirement. He said:[691]

> In cases such as the present it seems that plaintiffs will ordinarily be concerned about being identified in the context of the facts of a particular case to those who know them, but do not know the facts.

6.98 This is in line with the Privacy Act, which defines "personal information" as "information about an identifiable individual."[692]

6.99 Yet all this is not entirely plain sailing. In introducing the topic of identity in *Andrews*, Allan J said "*At least in most circumstances* in order to make out a claim a plaintiff will need to establish that he or she has been identified in the publication either directly or by implication."[693] The matter was also left open in *A v Hunt*.[694] There is one District Court case where identification was held not to be required. It is *L v G*,[695] where sexually-explicit photographs of a woman were published without her consent in an adult magazine. She was not identifiable in the pictures, but was nevertheless awarded damages for breach of privacy. Judge Abbott said the defendant's conduct had "violated the plaintiff's shield of privacy." In *Hosking*, Blanchard P and Gault J appeared to doubt the decision, saying it might have been better brought in breach of confidence.[696] If there

688 David A Elder *Privacy Torts* (Thomson West, Egan (MN), 2002) para 1.3.

689 It has been suggested that in Māori tradition deceased persons still possess some dignity and privacy that could be breached: Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press, Palmerston North, 2004) 57.

690 (13 December 2004) HC WN CIV 2004–485–1299-1300, para 7.

691 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576, para 60.

692 Privacy Act 1993, s 2.

693 *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004 404-3576, para 52 (emphasis added).

694 (17 May 2006) HC WN CIV 2003–485–2553.

695 [2002] DCR 234.

696 *Hosking v Runting* [2005] 1 NZLR 1, para 84.

is ever to be a tort of intrusion into solitude and seclusion where publication is not of the essence, the question of identity would not arise. The question remains open, however, of how essential it is in the publication tort.

Mental element

6.100 A final question which is not settled by *Hosking v Runting* is what, if any, mental element is required in the defendant. When the media are defendants, the question will arise seldom: publication is hardly ever anything but an intentional act, although one could perhaps imagine a case where an item which has been ordered to be withdrawn is left in the newspaper by mistake. The question will be more likely to arise if the defendant is someone other than the media. For example, imagine a person who has left sensitive information in an insecure place where it is stolen or accessed by someone else who publishes it. In such cases there might arise a question of whether negligence will ground an action for intrusion of privacy. A more serious question is what the liability would be of a library, bookseller, printer or internet service provider who is involved in the distribution of material without knowing, and perhaps without any reasonable means of knowing, what it contains. So the question might arise whether the act of publication must be intentional, whether negligence will suffice, or whether the liability is absolute in that no mental element is required at all. The last of these possibilities is unattractive.

6.101 With only one exception, the Canadian provinces require that, to be actionable, an invasion of privacy must be "wilful and without colour of right."[697] The one exception is the Manitoba statute, which requires that the defendant must have acted "substantially, unreasonably and without colour of right."[698]

CONCLUSION

6.102 In this country the tort of invasion of privacy is in its infancy. It remains liable to be changed, or even reversed, by the Supreme Court. It extends so far only to publicity given to private facts. In other words, it is about informational privacy, and specifically about disclosure of personal information. Whether the courts will ever be prepared to extend it to cover intrusion into solitude and seclusion – that is to say, to spatial privacy – or indeed to any other kind of privacy invasion is undetermined. In some cases which arise on the publication tort, the guidance provided in *Hosking* will be sufficient. Some cases will clearly lie on one side of the line or the other. There can be little quibble, for instance, with the decisions in *Morgan v TVNZ*[699] and *P v D*.[700] Yet we have seen in this chapter that there is considerable uncertainty about the application of some of the elements of *Hosking*, and there are unanswered questions. Cases are unlikely to arise frequently. Since 1985 there have to our knowledge been 17 (see appendix to this chapter), most of which provide little guidance for the future. So the law will develop slowly and the uncertainties will remain for a long time. It may no doubt be said that this is true of many other areas of law besides privacy, but given that privacy is a limitation on freedom of expression,

697 Privacy Act 1978 RSS c P-24, s 2; Privacy Act 1990 RSNL c P-22, s 3; Privacy Act 1996 RSBC c 373, s 1.

698 Privacy Act CCSM s P125, s 2.

699 (1 March 1990) HC CHCH CP 67/90.

700 [2000] 2 NZLR 591.

and that the uncertainties which attend the law at the moment are considerable, this must create a level of concern.[701] In this chapter we have attempted to identify some of the doubts. In summary they are as follows.

6.103 First, the core elements of the tort are not easy of application. There is still room for argument about whether the "highly offensive" test is appropriate. Assuming it is, there is inherent vagueness about the concepts of:

- reasonable expectation of privacy;
- highly offensive; and
- legitimate public concern.

6.104 All require the exercise of human judgement, and in all of them different individuals might disagree at the margins. No doubt this is true of many other legal concepts, but in privacy the uncertainties are very pronounced. Nicole Moreham has said that the highly offensive test:[702]

> often seems to operate as an appeal to the Judge's instinctive feeling about the seriousness of the intrusion … Indeed, it is difficult to see how a Judge could set out clear rules about what is particularly humiliating, distressing, or harmful to an objective reasonable person.

No doubt, as Moreham suggests, "highly offensive" is the most open-ended of the three, but the same criticism can be pointed at the other two as well. The grounding of the tort in human dignity does not greatly assist the decision-making process.

6.105 Secondly, there are difficult questions as to how a "reasonable expectation of privacy" applies in relation to public places, when there has been prior publication, when the plaintiff is a public figure or celebrity, or when the plaintiff has been culpable in some way or other.

6.106 Thirdly, there are doubts about the remedies:

- Although injunction is said to be an exceptional remedy, it is not clear how far protection of privacy will be seen to require more ready injunctive relief than in other publication torts, such as defamation.
- It is not clear how the measurement of damages is to be undertaken. The measurement of damage to dignity is in its infancy.
- It is not clear whether there may be other remedies such as orders for delivery of documents or account of profits.

6.107 Fourthly, the relationship of the tort to other causes of action such as defamation and breach of confidence needs to be worked through.

---

701 This was a major concern of the dissenters in *Hosking*: see *Hosking v Runting* [2005] 1 NZLR 1, paras 211 and 221 Keith J and para 270 Anderson J. See also *Bradley v Wingnut Films Ltd* [1993] 1 NZLR 415, 423 Gallen J.

702 NA Moreham "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation: Essays in Honour of John Burrows QC* (LexisNexis NZ, Wellington, 2008) 231, 246-247.

6.108 Fifthly, the range of possible defences remains to be explored. In *Hosking v Runting*, public concern was the only one itemised. Consent, privilege and contributory negligence are possibilities.

6.109 Sixthly, there are many unanswered questions:

- Does an action for breach of privacy lie in relation to false statements?
- Does the tort require publicity as opposed to publication?
- Are corporations able to sue?
- Can actions be brought by the living relatives of the deceased to protect the privacy of a deceased person?
- Does the plaintiff have to be identified, and if so identified to whom?
- Does the tort require a mental element, and if so what?

6.110 Given the inevitable paucity of litigation, the common law will take a long time to develop. In the next chapter we shall consider the question of reform.

Appendix to chapter 6

New Zealand tort cases with privacy as an ingredient of the cause of action

In the following New Zealand cases a tort of invasion of privacy, foreshadowed or actual, was an ingredient of the cause of action. In most of the pre-*Hosking* cases the existence of the tort was pleaded as "arguable", as a basis for an interim injunction. In most of the cases the privacy tort was pleaded as one of a number of alternative grounds.

Tucker v News Media Ownership Ltd [1986] 2 NZLR 716 (HC) McGechan J (man for whom money being raised to enable him to have cardiac surgery sought injunction to stop publication of fact that he had a prior criminal record: interim injunction granted, later discharged because of futility).

Morgan v Television New Zealand Ltd (1 March 1990) HC CH CP 67-90 Holland J (young girl subject of custody dispute sought injunction to stop broadcast of documentary about her life: interim injunction granted).

Re Morgan (15 March 1990) HC CH CP 93-90 (same material facts as above: interim injunction refused because newspaper already in course of distribution).

Marris v TV3 Networks Ltd (14 October 1991) HC WN CP 754-91 Neazor J (man sought interim injunction to stop broadcast of footage of a "door-step" interview: injunction refused because damages adequate remedy).

Moko-Mead v Independent Newspapers Ltd (25 October 1991) HC WN CP 813-91 Neazor J (man sought interim injunction to stop publication of allegation of sexual harassment: injunction refused on basis that the matter was one of public rather than private life, and on balance freedom of information prevailed).

C v Wilson & Horton Ltd (27 May 1992) HC AK CP 765-92 Williams J (man under investigation by Serious Fraud Office sought injunction to prevent publication of his name: interim injunction granted).

Hickmott v Television New Zealand Ltd (31 March 1993) HC AK CP 213-93 Robertson J (religious group sought interim injunction to stop broadcast relating to custody case: injunction refused on ground that the high threshold required to overcome freedom of information not reached, and a sanction was available under the Guardianship Act).

Bradley v Wingnut Films Ltd [1993] 1 NZLR 415 (HC) Gallen J (family sought injunction to stop image of tombstone being shown in "splatter" movie: injunction refused on basis that there was no private fact, and the depiction would not be highly offensive).

Beckett v TV3 Network Services Ltd [2000] NZAR 399 (HC) Robertson J (Police sought injunction to stop broadcast of item relating to death in a car park before coroner's inquest: injunction refused on basis that the facts were not private).

A v Wilson & Horton Ltd [2000] NZAR 428 (HC) Doogue and Robertson JJ (policeman who had shot a man in the street sought interim injunction to stop publication of his name: injunction refused on basis the fact was not private).

P v D [2000] 2 NZLR 591 (HC) Nicholson J (well-known professional person sought injunction to stop publication suggesting the person had been treated for mental illness: injunction granted on grounds that the criteria of the tort had been made out).

Abbott v The Christchurch Press Co Ltd (13 December 2002) HC CH T9-02 Chambers J (policeman who had shot man sought injunction to stop publication of his new identity and whereabouts: injunction granted).

L v G [2002] DCR 234 Judge Abbott (woman sought damages when pictures of her naked body published in adult magazine: $2500 damages awarded).

Hosking v Runting [2005] 1 NZLR 1 (CA) (couple sought injunction to stop publication of photographs of their infant children taken in a public place: injunction refused on basis that the facts were such that there was no reasonable expectation of privacy; nor was publication highly offensive).

Andrews v Television New Zealand Ltd (15 December 2006) HC AK CIV 2004-404-3536 Allan J (couple sought damages of $100,000 when broadcast programme showed them after they had been injured in a car accident, and played a recording of a conversation between them: damages refused on ground that the broadcast was not highly offensive).

Brown v Attorney-General [2006] DCR 630 Judge Spear (man released from prison, where he had served a sentence for child sex offences, claimed damages when police issued a flyer identifying him and the area in which he lived: damages of $25,000 awarded for invasion of privacy).

Rogers v Television New Zealand Ltd [2008] 2 NZLR 277 (SC) (man alleged to have confessed a murder to Police, but then acquitted after the confession was held inadmissible, sought injunction to stop broadcast of the "confession": injunction granted in High Court, but appeal allowed because statement made to Police was likely to have been presented in evidence in court, and thus was not a private fact).

Note: We understand there are at least two other cases where injunctions have been granted, but where the file has been sealed; details are thus not available.

Summary

Total number of cases: 17 (+ 2 uncertain)

Cases where injunction granted:	5
Cases where injunction denied:	9
Cases where damages awarded:	2
Cases where damages refused:	1

Chapter 7

Reform of the civil and criminal law on personal information disclosure

7.1 Having set out the current law relating to disclosure of personal information in Part 1, and examined the issues surrounding the tort of invasion of privacy in chapter 6, we now consider options for law reform in the area of privacy breaches involving information disclosure. The chapter is in two parts. The first part looks at possible reform of the *Hosking* tort, while the second part raises questions about whether there are any further gaps in the civil and criminal law in this area.

THE *HOSKING* TORT

7.2 In chapter 6 we analysed the tort of invasion of privacy as it currently stands in New Zealand. In this chapter we shall discuss whether reform is required. We emphasise that we are dealing in this chapter with the tort as it is currently formulated in *Hosking v Runting*: a tort of invasion of privacy by publicity given to private facts. We leave for chapter 11 consideration of whether there should be a further tort, or an expansion of this tort, which deals with intrusion into solitude and seclusion or prying into private affairs.

Should there be a tort at all?

7.3 The *Hosking* court was split three-two on whether there should be a tort at all. In *Rogers*[703] in the Supreme Court, Anderson J made it clear that he regards that question as still being open. The reasons of the dissenting Judges in *Hosking,* Keith and Anderson JJ, were in essence that the tort would be too uncertain; that in the United States where it has existed for 100 years it has produced very little result; that a court should be most reluctant to lay down the law in a way which goes beyond the specific privacy protections already enacted by Parliament; and that in deserving cases other rules of law can provide appropriate remedies.

703 *Rogers v Television New Zealand* [2008] 2 NZLR 78.

For those reasons they concluded that the tort would be an unjustifiable limitation on freedom of expression. We now examine in more detail the arguments for and against the existence of such a tort.

Arguments against a tort

7.4 Given its apparent basis in dignity the main harm against which the tort protects is humiliation and distress. Once upon a time such non-physical harm was regarded as too insubstantial to merit redress in a court of law. In 1973 the editors of *Salmond on Torts* said that such harm "may be too trivial, too indefinite or too difficult of proof for the legal suppression of it to be expedient or effective."[704] John Fleming in his book on tort in 1998 noted that one of the reasons that intrusion into privacy had so far not been accorded recognition by the courts, was that "We are here concerned primarily with injury in the shape of mental distress which has so frequently involved the fear of opening the door to fanciful claims."[705]

7.5 In recent times there has been an increasing tendency to compensate such damage, although sometimes it is parasitic on other types of loss. In 2005 Stephen Todd, writing about the law of negligence, was still able to say that in that branch of the law "mere upset, grief or distress does not give rise to any cause of action."[706] It is notable, too, that in the House of Lords it was recently held[707] that the tort of *Wilkinson v Downton* (the intentional infliction of harm) was not available for anything less than physical or psychiatric injury.[708] Some may therefore hold the view that it is anomalous for the law of tort to redress intangible losses by an action for breach of privacy. Moreover, given that in all but the most exceptional circumstances even the most serious personal injury is not compensatable at common law in this country, it may be thought curious that an action in the higher courts is available for breach of privacy. Those who hold that view may believe that some other form of redress is more appropriate than a tort action.

7.6 The new tort upsets the balance worked out over a long period by the tort of defamation. That balance asserted that if I published something about a person which affected his or her reputation, and which I could not prove true, I was liable in defamation; but if I published something about him or her which was true, however damaging it might be, I was under no liability at all. A person deserved no protection against publication of the truth. The new tort of invasion of privacy stands that principle on its head by providing that people can sue for the publication even of true statements about themselves provided

704 R F V Heuston (ed) *Salmond on Torts* (16 ed, Sweet & Maxwell, London, 1973) 14.

705 John G Fleming *The Law of Torts* (9 ed, LBC Information Services, North Ryde (NSW), 1998) 664.

706 Stephen Todd "Negligence: The Duty of Care" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 115, 158.

707 *Wainwright v Home Office* [2004] 2 AC 406, para 47.

708 Lord Hoffmann said that in cases where the intention to cause harm was imputed only, emotional distress was never enough, but left open the question of whether it might be enough if there was a deliberate intention to cause such harm. But he continued (at 47): "In institutions and workplaces all over the country, people constantly do and say things with the intention of causing distress and humiliation to others. This shows lack of consideration and appalling manners but I am not sure that the right way to deal with it is always by litigation."

the publication meets the criteria laid down in *Hosking v Runting*. It may be wondered whether society's expectations have changed so much as to require such a change of principle and such a shift in the boundaries of freedom of expression.

7.7 There already exists a range of methods of enforcing privacy in bodies other than the courts. Much was made of this by Keith J in his dissent in *Hosking v Runting*.[709] Principle 11 in the Privacy Act provides that an agency which holds personal information must not disclose it to anyone, unless it falls within one of the exceptions provided for in that principle.[710] The Privacy Commissioner, and sometimes the Human Rights Review Tribunal, can resolve complaints about the breach of that principle. It does not apply to the media in their news activities.[711] The Broadcasting Standards Authority determines complaints about breach of privacy by broadcasters, and can award damages of up to $5000 plus costs in appropriate cases.[712] The Press Council can hear complaints against newspapers and magazines, although its jurisdiction is voluntary and it cannot apply monetary sanctions. Given the existence of these other remedies, do we need as well the heavy machinery of the courts? Some might argue that that machinery is inappropriate to enforce what they would see as no more than considerate and respectful behaviour. They might argue also that if there are gaps in the lower-level enforcement methods it would be preferable to fill them, rather than resort to methods of enforcement in the higher courts.

7.8 It may be wondered whether the tort will be pressed into service often enough to merit its existence. Given the cost of bringing an action and (paradoxically) the public nature of court proceedings, who will the plaintiffs be? In Canada the statutes which exist in some of the provinces are very rarely used. Likewise, in the United States the "publicity to private facts" tort seldom results in a win for the plaintiff, especially against media defendants.[713] In New Zealand, where we have a comparatively responsible media, there are not many examples of serious invasions of privacy,[714] although it must of course be remembered that the reach of the tort extends beyond the media.

7.9 We have noted the uncertainties in the way the elements of the *Hosking* tort are framed, and indeed in the very concept of privacy itself.[715] There is so much difficulty of definition and so much room for subjective judgment that there is a danger that any such tort will slide into areas which are not privacy at all, but rather just bad taste, or offensiveness pure and simple. Some are still of the

709 [2005] 1 NZLR 1, para 207.

710 Privacy Act 1993, s 6, information privacy principle 11.

711 Privacy Act 1993, s 2, definition of "Agency".

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

713 See chapter 4 above.

714 See, in the context of defamation, the comments of the Court of Appeal in *Lange v Atkinson* [2000] 3NZLR 385, para 33 Tipping J: "Generalisations in this area are dangerous but it is possible to say that New Zealand has not encountered the worst excesses and irresponsibilities of the English national daily tabloids."

715 See chapter 6 above.

view that privacy will always be too vague to be a satisfactory basis for any legal rule. As such it can be an unjustified limitation on freedom of expression. That was the clear view of the dissenters in *Hosking v Runting*.[716] However, the majority in *Hosking* obviously disagreed.

7.10 There is perhaps a further argument arising from privacy's perceived basis in dignity. If there is a tort of invasion of privacy, why does the law of tort not also protect against abuse or denigration on grounds, for example, of religious belief, race or disability? Why, it might be said, should privacy be special?

Arguments for the tort

7.11 There are counter arguments for retaining the tort in some form, be it statutory or common law.

7.12 Some breaches of privacy are egregious, and merit serious redress. Examples can be found in some of the extravagances of the British tabloids.[717] The conduct of an individual posting intimate photographs or disclosures on the internet might well evoke a similar reaction. A breach of privacy may sometimes merit a monetary award higher than those which are currently available in the lower tribunals and indeed higher than would be appropriate for any tribunal to grant. Moreover, as we have seen, damages for breach of privacy need not be confined to dignitary awards. There could, for example, be cases where significant financial loss could arise from a breach of privacy, and where no other tort is available. There is no particular inconsistency in having a series of lower-level enforcement mechanisms alongside the option of a court action for serious infringements. As Tipping J said in *Hosking*:[718]

> In the absence of any express statement that the Privacy Act was designed to cover the whole field, Parliament can hardly have meant to stifle the ordinary function of the common law, which is to respond to issues presented to the court in what is considered to be the most appropriate way.

7.13 One of the most effective remedies for breach of privacy is injunction, and that is only available from a court. It is not correct to say that claims for injunction are likely to be exceptional: the majority of the claims in New Zealand since 1985 have been for this form of prior restraint, and so have the great majority of the English cases. As we showed in chapter 6, there are situations where injunctions are a far more effective remedy for breach of privacy than a monetary award. To stop the publication of private information before it happens is really the surest way of putting matters right. This is not to say, of course, that the higher courts need necessarily be the only bodies empowered to grant an injunction or some similar order. It is not unknown for tribunals to have such powers: already the Human Rights Review Tribunal has a statutory power to make an order restraining the defendant from continuing or repeating a breach.[719] But the existence of an injunctive power does assume the existence of a tort, or something like it.

716 [2005] 1 NZLR 1, paras 211 and 220 Keith J and para 270 Anderson J.

717 One example is *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB).

718 [2005] 1 NZLR 1, para 227.

719 Human Rights Act 1993, s 92I(1)(b); Privacy Act 1993, s 85(1)(b).

7.14 At the other extreme, if privacy, being a dignitary tort, is actionable without proof of damage, arguments based on the intangible nature of the loss fall to the ground. The tort could stand without the need for any damage, of any type, to be demonstrated. It would in that respect resemble trespass to the person, false imprisonment, and even defamation.

7.15 The tort was foreshadowed in New Zealand as early as 1985[720] and its existence has often been affirmed since then. It may be difficult to reverse that trend now. It would be turning the clock back.[721] Moreover, given the emphasis on privacy internationally, it may give an unfortunate signal to the international community. England, Ireland, continental European countries, the United States and some of the Canadian provinces all recognise such a civil action. In Australia the highest court has not ruled out the possibility of such an action developing there.[722] The Australian Law Reform Commission has recommended the enactment of a statutory cause of action for invasion of privacy. In this international setting it might be seen as a retrograde step to reverse our present direction unless the tort was to be replaced by something equally effective.

7.16 Even if there were to be no tort of invasion of privacy, other existing causes of action would probably be pressed into service to do similar work. As we made clear in chapter 2, breach of confidence in particular is capable of expanding into the vacuum. This point was clearly made by Randerson J at first instance in *Hosking v Runting*.[723] It has indeed been the modus operandi of the English courts. It can lead to unfortunate distortion.

Q1 Is there value in a tort of invasion of privacy by publicity given to private facts? If so, what is that value?

If the tort were to go, should it be replaced by something else?

7.17 If it were to be decided not to continue with the tort of invasion of privacy and if nothing were to replace it, we would be left with the lower levels of enforcement (that is, primarily, the Privacy Commissioner and Human Rights Review Tribunal, the Broadcasting Standards Authority and the Press Council) together with the court's ability, already mentioned, to fill a vacuum with other causes of action. Would that be enough? There are three difficulties.

7.18 First, when the common law fills vacuums it tends to use fictions and other artificiality to do so. That does not improve the law's accessibility. That is precisely why the majority of the Court of Appeal in *Hosking v Runting* did not want breach of confidence to be used for this purpose.

7.19 Secondly, the lower-level forms of enforcement provide only patchy coverage, in particular as regards the media. The Privacy Act principles do not apply to most of the media in their news activities. The Broadcasting Standards Authority deals only with complaints against broadcasters. The Press Council,

720 *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716.

721 See *Hosking v Runting* [2005] 1 NZLR 1, para 247 Tipping J.

722 See chapter 4.

723 [2003] 3 NZLR 385.

while it deals with print publications, has no ability to impose sanctions. Moreover, there has developed a new media – internet blogs, for example – over which neither the Press Council nor the BSA have any jurisdiction. So were the tort to be abandoned, there would be incomplete coverage in the lower-level modes of enforcement.

7.20 Thirdly, the remedies available under the lower-level modes of enforcement are likewise patchy and inconsistent. There is no provision for injunction. The Broadcasting Standards Authority can award damages of up to $5000, the Human Rights Review Tribunal up to $200,000 for cases within its jurisdiction.

7.21 So, then, if it is felt that the tort should be abandoned, one would be left with a system without much coherence. The question might then arise whether one should expand the jurisdiction of some of the lower-level regulators. For example, should one confer on a body such as the Human Rights Review Tribunal the power to deal with a wider range of privacy issues than is now the case and enhance its repertoire of remedies? Or should one consider a new, specialist privacy tribunal? Yet to do this would effectively amount to the creation of a statutory tort at a lower level than the current one, enforceable by a tribunal rather than a court. This would signal that privacy is worthy of legal protection, but would relegate it to a level below that of the higher courts. The process would be more informal, and, it is to be hoped, cheaper. A ceiling could perhaps be put on damages, although some tribunals are currently able to award significant sums: the Human Rights Review Tribunal has the same limit as the District Court ($200,000), and the Weathertight Homes Tribunal has no statutory limit. The question is how far society would see the transfer of the courts' privacy jurisdiction to a tribunal as a devaluation of the currency of privacy, and whether it would accept it.

Q2 Do you think it would be sensible to abolish the tort without replacing it? If it is to be replaced, what should replace it?

If the tort is retained, should it be common law or statute?

7.22 In the last chapter we identified some uncertainties, gaps and problems with the *Hosking* tort. If it is decided to retain the tort, the question is whether one should live with those limitations and leave it to the common law to grow and develop, or whether one should codify the tort – in other words replace the common law by a statutory cause of action. The respective virtues of common law and statute as types of lawmaking have been much debated. Each camp has its adherents. Here we set out some of the arguments on each side.

Arguments for common law

7.23 Those who favour the retention of the common law tort would argue that common law method is fit for purpose in this area. Over the years as cases come before the courts the decisions on those cases will increasingly remove uncertainty by clarifying the elements of the tort and filling the gaps. A body of law will grow, and increasingly decisions will become more predictable. In England, where the volume of litigation is higher than here, this is already

beginning to happen; in a recent paper delivered at a conference Eady J enunciated 14 principles which he said can be derived from the growing body of English case law.[724] This is the way of the common law, and we are familiar with it in many other areas of both tort and contract.

7.24 The common law keeps in touch with reality. The judges are not making law in a vacuum, but in response to actual fact situations. They are grounded in fact, not abstract theory. They can ensure that the law develops in a practical way. Moreover, privacy is much at the mercy of new developments, particularly in the area of technology. If the tort remains a common law one, Judges can confront these new developments as they arise, and adapt the law to deal with them.

7.25 Another argument for retaining the common law is that, inevitably, the wording of any statute which might be devised would to some extent have to be uncertain and open-ended. Phrases such as "reasonable expectation of privacy", "highly offensive", and "public concern", might well reappear. The Canadian statutes contain phrases which are similarly open-ended: the Acts of British Columbia, Newfoundland and Saskatchewan, for instance, provide that the degree of privacy to which a person is entitled is "that which is reasonable in the circumstances." The Manitoba statute declares that the tortfeasor is a person who "substantially, unreasonably and without claim of right violates the privacy of another person." The phrase "public interest" appears in all four statutes. In other words, the argument is that such is the nature of privacy it will never be possible to pin it down to a catalogue of finite and precise propositions. There will thus remain an area for judicial creativity which is not much less than that provided by the common law. Decisions on the statute may therefore be just as unpredictable.

7.26 If, on the other hand, it were to be possible to draft a statute more precisely, there is a danger that it might rigidify the law and inhibit flexibility in the face of new developments.

7.27 The common law tort has not so far attracted much litigation and by its nature is unlikely to. The experience of the Canadian provinces is that statute is unlikely to attract much more. Given the effort and cost involved in preparing legislation, one may ask whether it would be worthwhile.

Arguments for statute

7.28 On the other hand there are arguments for codifying the tort. For present purposes we shall continue to use the term "tort" in this context, although some prefer to speak of a "statutory cause of action."[725]

7.29 While any statute will inevitably contain some vague and open-ended standards, statute can always define its concepts with more precision than the common law without abandoning flexibility. One device for so doing is to give a non-exhaustive list of examples. Thus, three of the Canadian statutes, having laid down the

724 Hon David Eady "Privacy and the Media" (paper presented to Cardiff School of Journalism, 29 September 2007).

725 This is the preferred terminology of the Australian Law Reform Commission: see Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) ch 74.

general principle that it is a tort to violate the privacy of another person, provide that, without limiting the generality of that proposition, proof that there has been surveillance, listening to or recording of a conversation, use of a person's name of likeness or the use of letters, diaries or other personal documents is prima facie evidence of a violation of privacy.[726] Another device is to set out in the statute a list of considerations to be taken into account in determining whether the broad criteria have been met. Thus, the Saskatchewan statute provides that without limiting the generality of the earlier provisions, in determining whether any act, conduct or publication constitutes a violation of privacy, regard shall be given to:[727]

> (a) the nature, incidence and occasion of the act, conduct or publication
>
> (b) the effect of the act, conduct or publication on the health and welfare or the social, business or financial position of the person or his family or relatives,
>
> (c) any relationship whether domestic or otherwise between the parties to the action,
>
> (d) the conduct of the person and of the defendant both before and after the act, conduct or publication, including any apology or offer of amends made by the defendant.

The New South Wales Law Reform Commission lists in its consultation paper at least ten factors which may be relevant in determining whether there has been a reasonable expectation of privacy.[728] They include such things as the age of and relationship between the parties, whether any information disclosed consisted of sensitive or intimate private facts, and the manner in which such information was disclosed. Such a list of aids can be built up by the common law only after a very long period of time. Statute can do it straight away.

7.30 In the same way, statutes can fill obvious gaps in advance without waiting for litigation to arise. Thus, the Canadian statutes list matters of excuse and defence, including privilege, fair comment and consent.[729] Saskatchewan has a special defence for the news media.[730] Three of the statutes list the range of possible remedies, including account of profits and orders to deliver up documents.[731] Three of them also provide that actions for violation of privacy are extinguished by the death of the individual whose privacy is alleged to have been violated.[732] The New South Wales Law Reform Commission consultation paper notes a number of issues that legislation should address, including whether fault is necessary, whether damage should be an element, whether the cause of action should be limited to natural persons, and the effect of death on a cause of action.[733] In other words, while one may have to wait

726 Privacy Act CCSM s P125, s 3; Privacy Act 1978 RSS c P-24, s 3; Privacy Act 1990 RSNL c P-22, s 4;

727 Privacy Act 1978 RSS c P-24, s 6(2).

728 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP 1, Sydney, 2007) 7-11.

729 Privacy Act CCSM s P125, s 5; Privacy Act 1978 RSS c P-24, s 4; Privacy Act 1990 RSNL c P-22, s 5; Privacy Act 1996 RSBC c 373, s 2(2).

730 Privacy Act 1978 RSS c P-24, s 4(1)(e).

731 Privacy Act CCSM s P125, s 4; Privacy Act 1978 RSS c P-24, s 7; Privacy Act 1990 RSNL c P-22, s 6.

732 Privacy Act 1990 RSNL c P-22, s 11; Privacy Act 1978 RSS c P-24, s 10; Privacy Act 1996 RSBC c 373, s 5.

733 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP 1, Sydney, 2007) ch 7.

many years before the common law can provide definitive answers to these questions, statute can do it immediately. Given that many people have to regulate their conduct on the basis of the law, a degree of immediate certainty and predictability is attractive.

7.31 Privacy law has an impact on many sectors of society. The media are affected by it. So are law enforcement agencies, employers and the medical profession. As we showed in our 2008 study paper, there are many countervailing factors which must be placed in the balance when privacy protection is in question.[734] They include freedom of information, freedom of the press, health and safety issues, law enforcement issues, and many others. Judges, when they make decisions as to how the common law should develop, have access to far less information than Parliament does when it passes statutes. Judges listen mainly to legal argument, no doubt supplemented by evidence of common practice. They sometimes allow counsel for affected interests to appear, as they did in *Hosking v Runting* where counsel for media outlets and the Commissioner for Children appeared as interveners by leave. However, statutory lawmaking has access to more extensive consultation procedures, and thus to a much wider range of information and opinion, both in the course of preparing the Bill and at the Select Committee stage in Parliament. The supporters of statute would argue that, in matters of real social import such as privacy, the Parliamentary process has a better machinery for getting the balance right.

7.32 In the absence of much New Zealand authority the judges, if the common law is left to itself, will undoubtedly be referred to English and United States authority. Commentators on the law will be influenced by it, and New Zealand courts refer frequently to such commentary in the course of their decision-making. Yet authorities from those other jurisdictions may not be appropriate for New Zealand. The United Kingdom situation is heavily dependent on the European Convention of Human Rights and the English cases are influenced by European jurisprudence. The criterion of "highly offensive" does not apply there, except in marginal cases, and the European Convention contains protections for both privacy and freedom of expression, whereas in this country privacy is not expressly protected by our Bill of Rights Act. Already there is English authority about photographing children in a public place which runs directly counter to *Hosking*.[735] In the United States, by contrast, the constitutional guarantee of freedom of expression is given great weight and the media generally win cases on the publication tort.[736] In other words, the cultures of these other jurisdictions are different, and it is important that the law is developed here so as best to fit New Zealand's needs. When there are diverse precedents from a number of jurisdictions in the mix, there is always the danger that our jurisprudence may be influenced by them and begin to run in contradictory directions. Statute law is uniquely able to fashion a law for New Zealand.

734 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 185-191.

735 *Murray v Big Pictures UK Ltd* [2008] EWCA Civ 446.

736 See above, chapter 4

7.33 As we have noted, the law of privacy affects many people. Most of them are not lawyers. Statute, which can set out the law in its entirety in one place in a series of principled statements, is much more accessible to the uninitiated than the common law, which is located in the scattered judgments of the courts. Some would argue that this alone justifies codification, even if the resulting statute does little more than replicate the common law.

7.34 If it is decided to expand the tort, or create a new one, to cover intrusion into seclusion, solitude and private affairs, that would probably need to be done by a statute, because there is in this country no common law base on which to build, and because of the necessity of reconciling complex issues about the detection of crime. If that happens it would make sense to have a single Act combining both torts. There are links between the two: the defences may well be the same, and, as the BSA's jurisprudence demonstrates, the two types of infringement of privacy, disclosure and intrusion, are often combined.

Q3 If there is to be a tort, is it better to codify it in statute, or leave it to evolve by case law?

If there is to be a statute, what should it contain?

7.35 We seek views on what the content of a statute might be should there be a decision to move to a statutory tort. We ask this for two reasons. First, were the Commission to recommend such a statute it would be expected to recommend what its contents should be. Secondly, a consideration of what such a statute might contain will assist in determining the prior question of whether there should be a statute at all.

7.36 We emphasise again that in this section we are concerned only with the tort of invasion of privacy by the publication of private facts: in other words, the *Hosking* tort. We also note that, even if it were decided not to have a tort actionable in the courts, but instead a cause of action enforceable in court-level tribunals, a question would still arise as to how the elements of that cause of action might be defined. The questions we are about to ask would be relevant in that context as well.

7.37 In chapter 6 we analysed the existing tort and drew attention to its uncertainties, and the questions about it which still remain to be answered. The following questions are based on the analysis in that chapter, and paragraph references are to that chapter.

Q4 If there is to be a statute, what should it contain? It would be helpful if you answered the specific questions 5-23 below, but you need not confine yourself to those questions.

The elements of the tort

Q5 Should the "highly offensive" test remain as a separate element of the tort? (paras 6.52-6.61)

Q6 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? (paras 6.24-6.25)

Q7 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? (paras 6.27-6.32)

Q8 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? (paras 6.33-6.35)

Q9 In what circumstances can there be a reasonable expectation of privacy in relation to something which has already been published? (paras 6.40-6.42)

Q10 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? (para 6.43)

Q11 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? (paras 6.44-6.51)

The defence of legitimate public concern

Q12 Would it be helpful, in a statute, to give examples of matters which are normally of legitimate public concern? (paras 6.62-6.73)

Q13 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? (para 6.71)

Gaps in the present law

Q14 Other than legitimate "public concern", what defences should there be to a cause of action for publicity given to private facts? (paras 6.91-6.92)

Q15 What remedies should be available? (paras 6.74-6.82)

Q16 Is it possible, or desirable, to list considerations to be taken into account in assessing damages? (paras 6.74-6.76)

Q17 Should it be possible to obtain a remedy in this privacy tort (or cause of action) if some or all the statements made about the plaintiff are untrue? (paras 6.85-6.87)

Q18 Should wide publicity be required to ground a cause of action or might publication to a small group be enough in some cases? (para 6.89-6.90)

Q19 Should it ever be possible to obtain a remedy for invasion of the privacy of a deceased person? (paras 6.95-6.96)

Q20 Should corporations, or other artificial persons, be able to bring an action for invasion of privacy? (para 6.94)

Q21 Is it possible to lay down a statutory test to clarify the special position of children? (paras 6.36-6.39)

Q22 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? (paras 6.97-6.99)

Q23 What mental element should be required to found liability in a defendant? (paras 6.100-6.101)

Conclusion

7.38 In this section we have posed a series of questions about the future of the tort of invasion of privacy by publication of private facts. The shape of the tort, and indeed its very existence, have been the subject of differing opinions. There are divergent views on a number of key questions.

7.39 The Commission has not formed a view, and welcomes feedback from the public on the following sequential questions:

- Should there be such a tort at all?
- If there should not be a tort, what, if anything, should replace it? (Should there be a statutory cause of action enforceable at a lower level than the courts?)
- If there should be a tort, should it remain a common law tort, or should it be codified in statute?
- If there should be a statutory tort, what should the statute contain?

7.40 We have not considered whether there should be a tort of intrusion into solitude or seclusion. That will be discussed in chapter 11.

ARE THERE ANY FURTHER GAPS IN THE LAW RELATING TO DISCLOSURE OF PRIVATE INFORMATION?

7.41 In the earlier part of this chapter we discussed the possibilities of reform in the *Hosking* tort. In this section we examine whether other aspects of the law relating to disclosure of private information might be considered for reform. We are here concerned with the law in relation to the publication of information in respect of which there is an expectation of privacy. We shall deal with intrusion, surveillance and interference with spatial privacy in Part 3 of this issues paper.

Criminal offences

7.42 In chapter 2 we set out the criminal offences relating to personal information disclosure. In essence those offences can be classified into four groups.

7.43 First, there is information arising in judicial proceedings which is suppressed either automatically by statute or by order of the court or tribunal. We are not concerned with those provisions here because, while privacy is sometimes a relevant consideration, other factors drive such suppression orders. They include the need for a fair trial, the administration of justice, the reputation of individuals, and sometimes public morality.

7.44 Secondly, a number of statutory provisions prohibit the publication of information which has been obtained either illegally, or under a warrant which has been issued for a particular purpose. The offences include:

- disclosing the details of a communication obtained by an illegal interception;[737]
- disclosing details obtained from a bodily sample under the Criminal Investigations (Bodily Samples) Act 1995;[738]

737 Crimes Act 1961, s 216C.

738 Criminal Investigations (Bodily Samples) Act 1995, s 27.

- disclosing details of matter obtained by the use of an interception warrant under the Misuse of Drugs Act[739] or Crimes Act;[740] and
- the publication of film taken in breach of the intimate covert filming provisions of the Crimes Act.[741]

In these cases the prohibition on publication reinforces the prohibitions on obtaining the information or, in the case of a warrant, imposes sanctions to ensure that the information obtained is used only for the purpose for which the warrant was issued.

7.45 Thirdly, there are a number of provisions which protect information which has been acquired by, or provided to, a government agency for a particular purpose. Such provisions relate to:

- the details of census forms;[742]
- information held by electoral officers;[743]
- tax information held by the IRD;[744]
- remuneration information held by the Remuneration Authority;[745] and
- various types of health information.[746]

These provisions ensure that people who entrust private information to the authorities can be assured it will be used only for the purpose for which it was entrusted. Considerations of trust in Government are important, as is the necessity of obtaining public co-operation in the supply of such essential information. In other words, there are public interest factors at play in the recognition of these offences, as well as the need to ensure the privacy of the individual.

7.46 Fourthly, there are a very few provisions which prohibit disclosure of information simply because of its private nature and the effect its disclosure will have on the individual. The best example is the Criminal Records (Clean Slate) Act 2004 which prohibits the disclosure of convictions more than seven years old, where no sentence of imprisonment was imposed.[747] Even here protection of privacy is not the main purpose: rather it is rehabilitation.

7.47 The conclusion which we may draw from this is that, if we leave aside suppression in judicial proceedings, these provisions mainly protect information either because of the *way* it was obtained or the *reason for which* it was obtained. In this respect there is a clear analogy with the civil wrong of breach of confidence. In other words, there seems to be no policy of rendering criminal the publication

739 Misuse of Drugs Amendment Act 1978, s 23.

740 Crimes Act 1961, s 312K.

741 Crimes Act 1961, s 216J.

742 Statistics Act 1975, s 40.

743 Electoral Act 1993, s 116.

744 Tax Administration Act 1994, ss 143C and 143D.

745 Remuneration Authority Act 1977, s 9.

746 For example personal information acquired under the National Cervical Screening Programme (Health Act 1956, ss 112J, 112Y and 112Z) and information given to a Mortality Review Committee (New Zealand Public Health and Disability Act 2000, s 18(7)).

747 Even the intimate covert filming provisions require that the film be taken without the knowledge or consent of the person: it is the covert nature of the filming which is of the essence rather than the subject of the film.

of information on the sole ground that it is humiliating, embarrassing or distressing to the person concerned. Thus, if intimate photographs are taken of a person with his or her consent it appears to be no offence to publish them on the internet or elsewhere without that person's agreement.[748] It is the intrusive *taking* of the pictures which is the gravamen of the intimate covert filming offences, not just the intimate character of the image obtained. It may be noted in passing that this approach of the law is consistent with the fact that it is no longer a criminal offence even to publish seriously defamatory material.[749] We turn now to ask whether the criminal offence provisions need reform or amendment. There are four questions.

Are all the existing offences necessary?

7.48 In many cases the existing offences were enacted before the passage of the Privacy Act 1993. It could perhaps be argued that with that new method of enforcement the heavier hand of the criminal law is no longer needed in all cases. For example, should the disclosure of census information under the Statistics Act still remain an offence? Should it remain an offence under the Electoral Act to disclose voter details? One would need to consider whether the deterrence focus of the criminal law is still needed. It would, moreover, be necessary to examine the policy behind each individual provision, and the interests it protects, before one could confidently answer such a question. It may also be relevant whose conduct is in question: for example, an individual employee or an organisation.

Should there be more offences than there now are?

7.49 Some might possibly argue that it should be an offence in extreme cases to publish deeply private information without the consent of the person concerned. A photograph, for example, of a woman unclad in the shower taken with her knowledge and consent but published on the internet without that consent might be thought by some to be a case meriting the intervention of the criminal law. Situations have arisen in which intimate visual recordings are made with consent by partners in an intimate relationship, and then published (often on the internet) by one partner after the relationship ends. At present the only option in such cases for the person whose intimate images have been published without consent is to complain to the Privacy Commissioner (in which case the domestic affairs exception in section 56 of the Privacy Act may well prevent the complainant from obtaining a remedy), or to bring a tort claim for invasion of privacy.[750]

7.50 One question that might be considered in due course is whether the Privacy Act ought to contain offences for very serious breaches of its provisions. There is some international precedent for this. In the United Kingdom, it is an offence to obtain, disclose or procure the disclosure of personal information knowingly or recklessly, without the consent of the organisation

748 Unless they were deemed "objectionable" under the Films, Videos and Publications Classification Act 1993.

749 Defamation Act 1992, s 56 (abolition of criminal libel).

750 See for example *L v G* [2002] DCR 234; *H v McGowan and Nutype Accessories Ltd* (6 April 2001) HC AK CP 147-SW01 Anderson J, cited in Judge David Harvey *Internet.law.nz: Selected Issues* (2 ed, LexisNexis, Wellington 2005) 338-339.

holding the information.[751] The Australian Law Reform Commission has recommended that the Privacy Commissioner should have the power to seek a civil penalty in the courts where there is a serious or repeated interference with the privacy of an individual,[752] although it noted that submissions did not support the introduction of criminal penalties.[753]

7.51 Incorporating an offence provision into the Privacy Act would be one way of providing a general criminal penalty for breaches of informational privacy while ensuring that it is not too broad and general by tying it to breaches of specific parts of the Act, such as the information privacy principles, taking into account the exceptions to them. However, under the existing complaints mechanisms complainants can receive damages through the Human Rights Review Tribunal. There would presumably then need to be some additional public interest in punishing egregious breaches of privacy, or some particularly bad conduct by the defendant (such as recklessness or flagrant disregard for the victim's privacy), in order to justify also imposing a criminal penalty. Criminal penalties may also be inconsistent with the policy underlying the complaints system. We will consider this issue in more depth in our review of the Privacy Act, but would be interested now in views as to whether this is an option which should be considered.

7.52 There are other inconsistencies and gaps in the existing provisions, which could be filled. Why, for example, should it be an offence to disclose information discovered by opening someone's mail,[754] whereas it is not an offence to publish information discovered through accessing someone's computer without authority?[755] In the latter case the accessing itself is an offence, but not the publication. Are there any other anomalies?

Should inconsistencies in the existing offences be eliminated?

7.53 In relation to some of the publication offences, the offence is committed by anyone who publishes the information *knowing* it to have been wrongfully obtained,[756] in others either knowledge or *recklessness* is required,[757] in others it is only *knowing disclosure* that matters.[758] There are inconsistencies also as to the matters of excuse or defence which apply to the various offences. For example, it is only an offence to disclose the contents of someone's mail if it is done "without reasonable excuse";[759] on the other hand, the offence of disclosing information obtained by an interception device is subject to several quite specific defences such as that the disclosure is made in the course of a police investigation or in court proceedings.[760] Should these defences be standardised? Indeed,

751 Data Protection Act 1998 (UK), s 55.

752 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) R50-2.

753 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 50.40.

754 Postal Services Act 1998, s 20(2).

755 Crimes Act 1961, s 252.

756 See, eg, Crimes Act 1961, s 216C.

757 See, eg, Crimes Act 1961 s 216J.

758 Misuse of Drugs Amendment Act 1978, s 23.

759 Postal Services Act 1998, s 20(2).

760 Crimes Act 1961, s 216C(2).

should one consider having a single offence of publishing material which has been obtained by an unlawful invasion of privacy? As we have seen, it is a defence to the *Hosking* tort that the matter published was of legitimate public concern. Should a similarly broad formulation apply in the case of the criminal offences? Should there be a defence specifically related to the media in the course of their news activities? (That of course is currently the case under the Privacy Act 1993.)

Should inconsistencies in the existing penalties be eliminated?

7.54 There is currently quite a range of penalties for publishing material obtained by unlawful interception. There is in theory a maximum penalty of two years' imprisonment for publishing material obtained by an interception device.[761] For disclosing material obtained from someone's mail there is a maximum penalty of a $5000 fine or six months' imprisonment.[762] For disclosing a private communication obtained under an interception warrant under the Misuse of Drugs Act and Crimes Act the penalty is a fine of only $500.[763] At the very least one would have thought a degree of standardisation was warranted here.

Q24 Should the existing criminal offences relating to disclosure of personal information be examined to see whether they are all still needed? Are there any existing offences that are no longer needed?

Q25 Are any new criminal offences needed?

Q26 Is it worthy of consideration whether the Privacy Act 1993 should contain offences?

Q27 Should inconsistencies in the existing criminal offences and penalties be removed? If so, how?

Other civil remedies

7.55 We have discussed the tort of invasion of privacy as enunciated in *Hosking v Runting*. Whatever happens to that tort it may be worth asking whether there is room for other methods of civil redress. One possibility is to provide in legislation that a number of specific statutory duties be enforceable by civil action so that the remedies of damages and injunction would be available. In other words, one could provide for a number of specific torts of breach of statutory duty. As we intimated earlier in this paper, such remedies may already be available for breaches of some of the current statutory duties: there is some

761 Crimes Act 1961, s 216C(1).

762 Postal Services Act 1998, s 20(2).

763 Misuse of Drugs Amendment Act 1978, s 23(2); Crimes Act 1961, s 312K(2).

authority in Australia for this, at least so far as the remedy of injunction is concerned. But the general tort is unpredictable in operation; it is unclear how far it applies, and to what statutory provisions it currently attaches. That is unsatisfactory.

7.56 One might consider, therefore, providing in legislation that some of the current criminal offences are also enforceable by civil action, enabling the victim to obtain damages or an injunction. So, for example, a right of action might be conferred on persons of whom intimate photographs have been published,[764] or whose private conversations have been intercepted and published.[765] The advantages of this would be that the constituent element of the wrong would be clearly spelled out in the statute, and there would be none of the uncertainties which currently attend the general tort of breach of statutory duty. There could be no argument by way of double jeopardy, because civil action serves a different purpose from the criminal law. There might be some difficulty as to whether the defences to the civil action would mirror those available in the criminal proceedings, but that could presumably be spelled out in the statute rather than leaving it to be worked out by the courts as is currently the position with the general tort.

7.57 It might also be a question whether such civil actions would be appropriately brought in the ordinary courts, or whether they would be better located in the lower-level modes of enforcement. This is the same question we have already asked in relation to the *Hosking* tort.

7.58 We will be interested to know your views on these possibilities.

Q28 Are any other civil remedies in relation to disclosure of personal information needed? If so, should they be obtainable in the courts, or in some other forum?

764 Contrary to Crimes Act 1961, s 216J.

765 Contrary to Crimes Act 1961, s 216C.

Part 3

SURVEILLANCE AND OTHER INTRUSIONS

Chapter 8

Surveillance: background

8.1 In Stage 1 of this Review we considered developments in the technologies of surveillance, and discussed regulation of surveillance outside the law enforcement context with reference to a number of hypothetical examples.[766] We concluded that technological developments were transforming surveillance, while at the same time the legal framework for regulating surveillance was patchy and inconsistent. Our more detailed analysis of the law in this issues paper reinforces our view that there appears to be a case for a more comprehensive and consistent approach to regulating surveillance. This approach will need to be compatible with the regulatory framework for surveillance by law enforcement agencies. As we discuss further below, law enforcement surveillance has been covered in separate Law Commission report, and is the subject of a Bill that has been introduced in the Parliament.

8.2 This chapter looks at the definition and purposes of surveillance, and asks how useful three key distinctions are for analysing surveillance. The distinctions discussed are those between public and private places, mass and targeted surveillance, and covert and overt surveillance. We look briefly at some types and technologies of surveillance, then discuss some of its uses. While surveillance has beneficial uses, it can have negative effects, and these are also considered, along with the available evidence about public attitudes to surveillance.

DEFINING SURVEILLANCE

8.3 The term "surveillance" comes from the French "surveiller", meaning to watch over. Often it is used to refer to literal watching, either with the naked eye or with a camera, telescope or other device (including devices that may record rather than being used to watch in real time). It also commonly refers to covert listening and, by extension, it has come to be used to refer to a wide array of methods of monitoring, with or without technological assistance. The field of "surveillance studies" takes a very broad view of surveillance, which includes not only the direct observation of people but also the monitoring of individuals through their data.[767]

766 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 135-147, 209-214.

767 For an introduction to surveillance studies see David Lyon *Surveillance Studies: An Overview* (Polity Press, Cambridge, 2007).

8.4 For the purposes of our discussion in this issues paper, we will define surveillance as *the use of devices intentionally to monitor, observe or record people's actions or communications*.[768] This is a broad definition, and we do not suggest that it would be suitable for incorporation into law.

8.5 There are a number of points to make about our definition of surveillance:

- As the inclusion of the word "intentionally" indicates, surveillance is not merely casual or accidental observation: it is deliberate and purposeful.
- "Surveillance" tends to suggest monitoring people in a systematic and ongoing way. However, for the purposes of this discussion we will not exclude incidents in which a device is used on a single occasion to observe or record someone.
- Ultimately, people are the subjects of surveillance. We are not concerned here with monitoring of animals or weather patterns, for example. The immediate focus of surveillance may be on a place (such as a street or building) or an object (such as a vehicle), but the purpose of the surveillance will relate to the people who may enter that place or use that object.
- Monitoring can take a range of forms, including "listening to, watching, recording, or collecting … words, images, signals, data, movement, behaviour or activity".[769]

Use of devices

8.6 We have limited our definition to surveillance carried out by the use of devices, although we recognise that it is possible to monitor and observe people by means of a person's unaided senses. Intrusive watching and monitoring without the use of devices falls within the broader category of "intrusion", discussed in chapter 11. We restrict our consideration of surveillance to activity carried out using devices in part for pragmatic reasons: it makes it easier to identify the boundaries of any legal regime for controlling surveillance. The Hong Kong Law Reform Commission commented that it would be difficult to draft legislative provisions prohibiting surveillance carried out with the ordinary senses: "The necessary intent would be that of surveillance. Where devices are not deployed, problems of proof are likely to be acute. Reference to devices would facilitate proof."[770]

8.7 There are also a number of characteristics of surveillance using devices that distinguish it from observation using the unaided senses, and make it of particular concern:

768 Other useful definitions can be found in New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC No 98, Sydney, 2001) 55-58; Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006) 4; Roger Clarke "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (accessed 20 June 2008).

769 New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC No 98, Sydney, 2001) 58.

770 Law Reform Commission of Hong Kong *Privacy: Regulating Surveillance and the Interception of Communications* (Consultation Paper, 1996) 33.

- By enhancing ordinary senses, surveillance devices allow people to see and hear things, and learn information about others (such as their location), in a way that would simply not be possible otherwise.
- Surveillance devices allow people to observe and monitor others without the knowledge of those who are under observation.
- Surveillance devices allow the actions and communications of others to be recorded. Although records can also be created by people writing down what they see or hear, records created using devices have at least the appearance of greater accuracy, and create particular risks (discussed under "Negative effects of surveillance" below).

Data surveillance

8.8 Our broad definition of surveillance would encompass monitoring people by monitoring data about them, whether that data is generated by themselves or by others. Australian academic Roger Clarke has coined the term "dataveillance" for this form of surveillance, particularly where it is automated and carried out by means of information technology.[771] In *Privacy: Concepts and Issues* we discussed ways in which advances in computer technology are making it easier to collect, store, combine and analyse data. We noted that everyday transactions (such as use of credit cards, bank cards, loyalty cards, mobile phones and the internet) leave a trail of digital data that can be analysed to develop profiles of people.[772] Such profiling can be seen as a form of surveillance, since it involves the use of devices to monitor people.

8.9 Protection of personal data is the focus of the Privacy Act 1993, which we will be reviewing in Stage 4 of this Review, so we do not intend to examine it in detail here. However, it can be difficult to draw a clear line between direct observation of individuals and monitoring of their data. A useful distinction can be drawn between routine collection and use of personal data, and the obtaining of personal information by the covert use of devices or software. We will include the latter type of data surveillance in this issues paper. Covert data surveillance can include recording data as it is being entered, intercepting data as it is being transmitted, or "hacking" into computer databases containing personal information.[773]

771 Roger Clarke "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (accessed 20 June 2008).

772 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 122-126. For more on the ways in which data is combined and analysed see Stephen Baker *The Numerati* (Houghton Mifflin, Boston, 2008).

773 New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC No 98, Sydney, 2001) 73-76.

PURPOSES OF SURVEILLANCE

8.10 Our definition of surveillance, unlike some others,[774] does not include the purpose of surveillance as part of the definition. We have, however, said that surveillance is purposeful. In our view, there are three high-level purposes for which surveillance is used: obtaining information, influencing behaviour, and seeking pleasure or gratification (voyeurism). We discuss the specific ways in which surveillance is used in a later section of this chapter.

8.11 Obtaining information is the primary purpose of most surveillance, which is why surveillance can be an interference with both informational and spatial privacy. Sometimes the information is received in real time for the purposes of making immediate decisions. For example, if a person has a camera outside her front door, she can see who is at the door and decide whether or not to open the door to visitors. Often, the information is recorded and stored, at least for a time. There can be a range of specific purposes for which information is collected by means of surveillance, including:

- gathering evidence of wrongdoing;
- documenting events or transactions;
- monitoring performance; and
- determining preferences (particularly of consumers).

8.12 The knowledge that they are, or could be, being watched can cause people to modify their behaviour. They may be deterred from acting in ways that are illegal or otherwise subject to social sanction or disapproval if they know or suspect that someone is watching or recording them. Furthermore, because many people find it unpleasant to be the subject of focused observation and monitoring, surveillance can be used to put pressure on people to act, or cease acting, in certain ways. Thus, influencing behaviour is another important purpose for carrying out surveillance, and is often combined with collection of information. For example, speed cameras are used to detect and identify speeding motorists, but they are also intended to deter people from speeding in the first place. In some cases there may be ambiguity about whether the surveillance is being used primarily for information collection or deterrence.[775]

8.13 Voyeurism is the third, and most specific, of the high-level purposes for which surveillance is carried out. Strictly speaking, a voyeur is someone who surreptitiously observes other people in intimate situations in order to gain sexual gratification.[776] More broadly, voyeurism could be defined as taking

774 For example, the NSW Law Reform Commission's definition states that surveillance is "for the purpose of obtaining information about a person who is the subject of the surveillance", while the Surveillance Studies Network says that surveillance is carried out "for the sake of control, entitlement, management, influence or protection": New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC No 98, Sydney, 2001) 58; Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006) 4.

775 For example, there have been cases of companies hiring security guards or others to videotape people protesting against the companies' activities. In such cases, the protesters may feel that the surveillance is being carried out for the purpose of intimidating them, while the company may say that the purpose is to provide evidence for use in possible legal proceedings. See *Local Residents Complain About Videotaping by Property Developer* [2006] NZPrivCmr 14 – Case Note 71808; Anna Mehler Paperny "BCTC Continues Surveillance Even as Privacy Probe Launched" (13 June 2008) *Globe and Mail* Toronto www.theglobeandmail.com (accessed 16 June 2008).

776 See discussion in New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) 11-13; Jonathan M Metzl "Voyeur Nation? Changing Definitions of Voyeurism, 1950-2004" (2004) 12 Harvard Review of Psychiatry 127.

pleasure in observing others while remaining unobserved. Such observation is sufficiently deliberate and purposeful to fall within our definition of surveillance. Voyeurs are not primarily interested in finding out information about those they observe or in influencing their behaviour. Only a very small percentage of surveillance will be motivated by genuine voyeurism, but there can be elements of voyeurism in surveillance ostensibly undertaken for other reasons.

SOME KEY DISTINCTIONS

8.14 There are a number of ways in which different types of surveillance can be distinguished from each other. We examine three key distinctions which could be relevant in developing a legal regime for controlling surveillance.

Public and private places

8.15 Some people take the view that the law should treat surveillance differently depending on whether the activity that is under observation is occurring in a public or a private place. Often those who subscribe to this view consider that no controls are needed on surveillance in public places, particularly where visual surveillance is concerned. For example, in its 1983 report on *Privacy*, the Australian Law Reform Commission wrote that:[777]

> It is not desirable, nor would it be feasible, to regulate the use of surveillance or recording by means of optical devices in streets, parks and other such entirely public places. To do so would put at risk all forms of outdoor photography and use of binoculars and telescopes, even the most innocuous. People who are in a public place must anticipate that they may be seen, and perhaps recorded, and must modify their behaviour accordingly. That is the essence of a "public" place.

Similarly, the United States Supreme Court, in a case concerning the use of a tracking device to follow a suspect's movements, held that:[778]

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the target of the tracking device] traveled over the public streets, he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

8.16 There are a number of assumptions underlying this view:

- A person in a public place can expect to be observed by others, and therefore cannot have a reasonable expectation of privacy.
- The use of devices to observe or record people in public places is no different from the use of an observer's unaided senses.
- People enter public places voluntarily, and thereby impliedly consent to being observed or recorded by others.
- People in public places know that they can be observed, and are responsible for modifying their behaviour accordingly.

777 Australian Law Reform Commission *Privacy* (vol 2, ALRC No 22, Australian Government Publishing Service, Canberra, 1983) 75.

778 *United States v Knotts* (1983) 460 US 276, 281-282.

8.17 Other commentators argue that people do not give up all expectations of privacy when they are in public, and that some regulation of surveillance in public places is needed.[779] They make the points that:

- People in public places still have some reasonable expectations of privacy and anonymity. They expect to be observed only casually and by a limited number of people; they do not expect to be the subjects of targeted or focused scrutiny, or to be recorded and have information about them disseminated to a wider audience.
- The use of surveillance devices is fundamentally different from unaided observation. As we mentioned above, it allows observers to see, hear and learn things that could not be observed with the ordinary senses; to monitor or observe others without their knowledge; and to record the actions and communications of others.
- It is an oversimplification to say that people enter public places voluntarily. As Andrew McClurg points out, "Merely to survive in society requires that people spend a considerable amount of their time in places accessible to the public."[780] Economic and social factors also mean that some (such as homeless people and young people) spend more of their time in public and semi-public places than others who have the means to keep themselves secluded for much of the time.
- There is no simple dichotomy between public and private places. Rather, there is a spectrum from private dwelling places at one end to truly open spaces such as public streets or parks to which everyone has access at the other.

8.18 The location in which a person is subject to surveillance is clearly relevant to the intrusiveness of that surveillance, and to the person's reasonable expectations of privacy. Debate focuses on the extent to which a strict division between public and private places either can or should be drawn for the purposes of developing legal controls on surveillance.

8.19 The distinction between public and private places may be more useful with respect to some forms of surveillance than others, and is probably most relevant to visual surveillance. It would clearly not be reasonable to stop people filming or taking photographs in public places as a general rule. However, there may be some situations in which visual surveillance in public places is sufficiently offensive to warrant some form of legal intervention. It may also be that some forms of visual surveillance in private places warrant criminal sanctions, whereas routine visual surveillance in public (such as use of video surveillance cameras) is most appropriately controlled within a regulatory framework such as that of the Privacy Act. At the same time, it would appear that the distinction between public and private places is not appropriate for some forms of surveillance. In particular, it would be almost pointless to restrict control of tracking devices to their use in private places. It would be unduly restrictive to say, for example, that a person cannot be tracked as he or she moves from one room to another of a private house, but that his or her much more significant movements across

779 See Andrew Jay McClurg "Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places" (1995) 73 NCL Rev 989; Elizabeth Paton-Simpson "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 U Toronto LJ 305; New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC No 98, Sydney, 2001) 46-51.

780 Andrew Jay McClurg "Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places" (1995) 73 NCL Rev 989, 1040.

town can be tracked freely. The Search and Surveillance Powers Bill 2008 takes the approach of distinguishing between different types of surveillance. Law enforcement officers will require a warrant for use of an interception or tracking device in any location, but will only require a warrant for visual surveillance of private activity in a private building or the curtilage of a private building.[781]

Targeted and mass surveillance

8.20 Targeted surveillance is focused on an identified person or persons, while mass surveillance casts the net more widely with the intention of identifying persons of interest.[782] Mass surveillance could be directed at a particular place (for example, a camera trained on a shopping street), or a particular group (for example, air travellers or employees of a particular business). Like all surveillance it is deliberate and purposeful, and while it does not have identified targets it could be looking for identified behaviours, for example. The distinction between targeted and mass surveillance relates closely to the distinction between covert and overt surveillance.

8.21 In general, targeted surveillance may lend itself more readily to remedies such as criminal prosecutions, or civil claims by the targets of the surveillance. Because it is systemic and not focused on particular individuals, mass surveillance may often be more suited to systemic regulatory responses such as rules or guidelines about how it should be conducted. However, some voyeuristic forms of mass surveillance (for example, placing a hidden camera in a public toilet or changing room) are suited to criminal sanctions or civil liability.

8.22 As with the public/private and overt/covert distinctions, the distinction between mass and targeted surveillance blurs at the edges. Mass surveillance can lead to targeted surveillance if it results in the identification of individuals of interest. In addition, data mining and other sophisticated techniques for analysing data mean that it is increasingly possible to sift through mass data to find information about particular individuals.[783]

Covert and overt surveillance

8.23 Covert surveillance occurs secretly, without the knowledge of the subject, while overt surveillance takes place openly, in circumstances in which the subject knows, or could reasonably be expected to know, that it is taking place. As we discuss below, however, a distinction based on the subject's knowledge that he or she is under surveillance is by no means straightforward. There is considerable overlap between the covert/overt and the targeted/mass surveillance distinctions. Covert surveillance will often be targeted, whereas overt surveillance does not usually have specific targets. Overt surveillance usually occurs in public places, although it can also occur in the workplace, whose position in terms of the public/private divide is somewhat ambiguous. Covert surveillance may take place in a range of public and private locations.

781 Search and Surveillance Powers Bill 2008, no 300-1, cl 46.

782 Roger Clarke "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (accessed 20 June 2008); Liberty *Overlooked: Surveillance and Personal Privacy in Modern Britain* (2007) 16.

783 Liberty *Overlooked: Surveillance and Personal Privacy in Modern Britain* (2007) 17.

8.24 In general, overt surveillance can be considered less invasive of privacy than covert surveillance. If people know that surveillance is operating in a particular place, they can choose to modify their behaviour. In theory, they can also avoid that place if they wish to, although as the use of surveillance becomes more common it becomes harder to avoid places where it is operating. By contrast, if people are unaware that they are being observed or monitored, they are prevented from taking steps to protect themselves and their privacy. Covert surveillance can catch people doing things they do not want others to see or know about, saying things that they want to be heard only by those they trust or with whom they are intimate, and revealing personal information that they wish to keep private. Covert surveillance can also leave people feeling insecure and violated if they find out that they have been secretly observed.

8.25 However, while covert surveillance may constitute the more serious invasion of privacy on the whole, it would be wrong to conclude that overt surveillance is free from problems or that there is no case for regulating it. To take matters to an extreme, few people would be comfortable living in a world in which everyone knew that they were under surveillance at all times. If overt surveillance (particularly visual surveillance) continues to become more widespread, and therefore more difficult to avoid, it will become all the more important to regulate it. As we have noted above, one of the purposes of surveillance is to influence people to modify their behaviour. It can be used to deter antisocial behaviour, but also to intimidate. The potential "chilling effect" of surveillance (discussed further below) is one reason for ensuring that there are some controls on its use. This effect clearly applies mainly to overt surveillance, since people will not modify their behaviour if they do not know that they are being observed (although they may do so if they have reason to believe that they may be under covert surveillance).

8.26 The distinction between overt and covert surveillance is an imperfect one, and the division is not always clear-cut. We have indicated that the distinction between overt and covert surveillance is based on whether the subject knows, or could reasonably be expected to know, that the surveillance is taking place. In practice, however, a distinction based on the subject's knowledge leaves many grey areas. For example, surveillance cameras may be visible, but that does not mean that people are aware of them.[784] An alternative way of thinking about the overt/covert distinction is to focus on whether those carrying out the surveillance are acting openly, with no intention to hide the surveillance devices (overt surveillance), or secretly, by attempting to hide the devices or disguise their purpose (covert surveillance). A distinction based on the intentions of those carrying out the surveillance will also be problematic, however, as those intentions will not always be clear.

784 Elizabeth Binning "Cameras Watch the City Almost Undetected" (30 June 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 30 June 2008).

8.27 Another problem with the overt/covert distinction is that it applies only at the point at which the initial surveillance is undertaken. Information gathered through overt surveillance can subsequently be used and analysed in ways that the subject of the surveillance knows nothing about.

How useful are these distinctions?

8.28 The three distinctions discussed above overlap to a considerable extent, and should not necessarily be viewed as alternatives. How useful each one is may depend on the particular type of surveillance under consideration, and the purpose of that surveillance. Each presents problems of definition and of drawing boundaries. However, these problems may be overcome to some extent by providing definitions by statute. For example, the Search and Surveillance Powers Bill provides definitions of "private building" and "non-private building".[785] Likewise, the definitional issues relating to the overt/covert distinction could be addressed by requiring notice of overt surveillance, as the New South Wales Law Reform Commission proposed. Where suitable notice is provided the surveillance would be deemed overt, and any other surveillance would be deemed covert.[786]

Q29 How useful are the distinctions between public and private places, mass and targeted surveillance, and overt and covert surveillance, for the purpose of framing laws to control surveillance? Are there any other key distinctions the Commission should consider?

TYPES OF SURVEILLANCE

Watching and visual recording

8.29 Visual surveillance devices such as cameras, video recorders and binoculars can be used in a range of ways, including to:

- watch or record people in public as they walk down the street or go about their daily business;
- observe or record people in places they expect to be private (such as their homes) from an external vantage point;
- watch or record people in private spaces, in workplaces, or in public settings, using hidden cameras located within those places;
- observe people's computer use, including access and passwords, through the use of hidden surveillance cameras or the conversion of webcams into surveillance devices; and
- make voyeuristic visual recordings of people in places where they do not expect to be photographed or recorded.

785 Search and Surveillance Powers Bill 2008, no 300-1, cl 3.

786 New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC No 98, Sydney, 2001) 78-85.

Listening and intercepting

8.30 Audio surveillance and interception devices can be used to:

- bug private homes, workplaces, and public spaces;
- record other people's conversations;
- record one's own conversations with others;
- intercept telephone conversations using various technologies (including VoIP[787] services such as Skype);
- intercept email and text messages; and
- intercept computer data.[788]

Locating and tracking

8.31 People's locations can be tracked in a variety of ways, including:

- placing Global Positioning System (GPS) location devices on people, or in vehicles or other objects;
- using the location data generated by cellphones and held by cellphone network providers;
- tracking people or their cars via networks of security and traffic cameras; and
- using Radio Frequency Identification (RFID) tags in identification documents such as passports or in consumer products to track people through scanning the RFID tags in the items they wear or carry.

Monitoring data

8.32 Examples of data surveillance by devices that covertly monitor or copy people's personal data include:

- using a computer to hack into someone's else's computer;
- installing spy software on someone else's computer;
- using keystroke loggers or hidden surveillance cameras to monitor data inputs into a computer, including passwords; and
- skimming an RFID chip with an RFID reader to collect information stored on the chip without the carrier's knowledge or consent.

TECHNOLOGIES OF SURVEILLANCE

8.33 New technologies are changing the nature of surveillance, and enabling it to become more pervasive. In *Privacy: Concepts and Issues* we discussed some of the trends in surveillance technologies:[789]

- Surveillance devices are becoming smaller, cheaper, less noticeable and easier to use. One consequence of this is the "democratisation" of surveillance, as ordinary citizens can more easily own devices capable of being used for surveillance.
- Information captured by surveillance technologies is being digitised, making it possible to combine it with other sources of digital data, analyse it in new ways, and disseminate it widely (particularly via the internet).

787 Voice over Internet Protocol that enables spoken conversations to be conducted in real time over the internet.

788 See New Zealand Law Commission *Computer Misuse* (NZLC R54, Wellington, 1999) para 18, for descriptions of methods for intercepting electronic data, such as packet sniffing.

789 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 136-139.

- Technological convergence is taking place: a device can be used for multiple purposes, or can form part of a larger integrated surveillance network.
- As a result of the above developments, surveillance is becoming more pervasive in everyday life. We could be moving towards "a 'digitally saturated world' in which surveillance sensors are placed or carried virtually everywhere … and are continuously and routinely gathering and storing information".[790]

8.34 We also looked at some developments in particular technologies:[791]

- *Closed circuit television (CCTV)* cameras are being more widely used in many countries, including New Zealand. Although the term CCTV is still commonly used to describe them, today's surveillance cameras are increasingly networked digital cameras rather than being strictly "closed circuit".[792] Some cameras are also starting to be equipped with new features, such as facial-recognition software that makes it possible to identify and track individuals,[793] microphones that allow eavesdropping on conversations, or speakers that allow messages to be addressed to people engaging in disorderly behaviour. Alongside these developments there are advances in the ability to analyse digital visual information, which in the future is likely to become indexable and searchable on the basis of images alone (that is, without the need for images to be linked to text).[794]
- Other developments in *visual surveillance* include research on mobile devices such as "robotic fliers" equipped with cameras; the ubiquity of cameras in cellphones; and the increasing popularity of webcams, allowing places or people to be monitored via the internet.
- *Radio-frequency identification (RFID)* technology can be used for a variety of purposes, including tracking people by means of RFID tags in objects carried or used by the person, or even by means of an RFID chip implanted under the skin.
- *Location technologies* such as the Global Positioning System (GPS) transmit satellite or other signals to a receiver, making it possible to determine where the person with the receiver is at any given time. Although GPS is not a tracking system, GPS receivers can be modified to become tracking devices by equipping them with wireless transmitters, thereby allowing third parties to remotely monitor the receiver's location.[795] An ordinary cellphone can also identify the location of its user, since cellphones regularly communicate their location to a base station.

---

790 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 137, citing Yves Punie, Sabine Delaitre, Ioannis Maghiros & David Wright (eds) *Dark Scenarios in Ambient Intelligence: Highlighting Risks and Vulnerabilities* (report of the SWAMI consortium to the European Commission, 2005) 6.

791 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 140-151.

792 For example, a wireless digital surveillance camera network has recently been installed in Newmarket in Auckland: Newmarket Business Association "Newmarket Launches State-of-the Art CCTV Network" (16 June 2008) Press Release; Ulrika Hedquist "Police and Public to Share Newmarket Wi-Fi" (23 June 2008) *Computerworld* New Zealand 9.

793 David Rowan "Let's Face it, Soon Big Brother will have No Trouble Recognising You" (13 January 2009) *The Times* www.timesonline.co.uk (accessed 15 January 2009).

794 James Vlahos "Surveillance Society: New High-Tech Cameras Are Watching You" (January 2008) *Popular Mechanics* www.popularmechanics.com (accessed 15 December 2008).

795 Renée McDonald Hutchins "Tied up in *Knotts*? GPS Technology and the Fourth Amendment" (2007) 55 UCLA L Rev 409, 418.

- *Biometric technologies* such as finger scanning and facial recognition are used to identify individuals or to verify their identity by means of their physical features. Some can be used covertly and at a distance, and in addition to their use in identification they may give clues as to what a person is thinking or feeling.
- *Spyware* is computer software that is secretly installed on a computer or other electronic device, such as a cellphone, that enables a third party to view or capture information, bandwidth or processing capacity from the computer or device without the permission or knowledge of the user and for a malicious or harmful purpose. Spyware can be used to collect personal information such as name, address, credit card or other financial personal details. It can also be used to collect information such as Web-surfing habits.[796]
- New forms of surveillance may raise privacy issues in future. For example, *brain scanning* is still developing. It currently requires a person to sit in the scanner for hours at a time, and needs to be adapted for each individual. However, it is not inconceivable that in the more distant future brain-scanning devices may be available that can be used quickly and from afar.[797] Likewise, *olfactory surveillance* may take new forms if devices are developed that can detect and analyse odours in ways that mimic but improve on the scent-detection capabilities of humans and other animals.[798]

8.35 Above all, it is the use of such technologies in combination with each other and with the analytical power of networked computing that has major implications for privacy. The result of convergence and networking has been described as the "new surveillance":[799]

> Compared to traditional surveillance, the new surveillance is less visible and more continuous in time and space, provides fewer opportunities for targets to object to or prevent the surveillance, is greater in analytical power, produces data that are more enduring, is disseminated faster and more widely, and is less expensive … Essentially all of these changes represent additional surveillance capabilities for lower cost, and exploitation of these changes would bode ill for the protection of privacy.

8.36 At the same time, it is important not to exaggerate the capabilities of surveillance systems. Whatever their future potential, at present they have significant technical limitations that act as a check on the ability of users of these systems to intrude on privacy.[800] For example, facial-recognition technology is still very

796 Australian Government, Department of Communications, Information Technology and the Arts *Spyware Discussion Paper* (May-June 2005) 6-7.

797 Roger Highfield "Mind Reading Device is Now a Possibility" (5 March 2008) and "Mind Reading by MRI Scan Raises 'Mental Privacy' Issue" (9 June 2008) *Telegraph* www.telegraph.co.uk (accessed 10 June 2008); "How Technology May Soon 'Read' Your Mind" (4 January 2009) www.cbsnews.com (accessed 6 January 2009).

798 Amber Marks "Smells Suspicious" (31 March 2008) *Guardian* www.guardian.co.uk (accessed 15 April 2008).

799 National Research Council of the National Academies *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washington, DC, 2007) 101-102.

800 National Research Council of the National Academies *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washington, DC, 2007) 116-118.

poor at picking individuals out of crowds, and at recognising faces at different angles or under different lighting conditions. Moreover, the accumulation of data through surveillance may outpace the capacity to analyse it.[801]

8.37 It is also possible that there could be technological solutions to some of the privacy problems that have been identified with particular technologies.[802] For example, video surveillance footage can be scrambled so that parts of the image such as faces are blurred, but can be unscrambled by authorised persons with a decryption key; and RFID tags can be made more privacy-friendly by deactivating them on purchase of the item to which they are attached, encrypting data held on them, or "clipping" them so that they can only be scanned at close range. Technical solutions such as these are not a complete answer to the problems of surveillance, but they may have an important role to play. Privacy-enhancing technologies can both complement law reform and be part of the regulatory toolbox: for example, the law could specify that particular types of privacy-enhancing technology are to be included as part of certain products or services.

Q30 Are there particular surveillance technologies that you are especially concerned about?

Q31 What role do you see for privacy-enhancing technologies in addressing the problems of surveillance? Is there a role for the law in promoting or mandating such technologies?

USES OF SURVEILLANCE

8.38 Surveillance has many specific uses, and can be used in many different contexts. While there may be disagreement about the legitimacy and usefulness of some of these uses, almost everyone would probably agree that surveillance can play a socially-beneficial role in particular circumstances. In this section we examine some of the ways in which surveillance is used. The use of surveillance by the media, by private investigators, and in the workplace is discussed in chapter 12.

Intelligence agencies

8.39 The surveillance activities of the intelligence agencies, particularly the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB), are outside the scope of our Review. Both the NZSIS and GCSB operate under statute.[803]

801 Cory Doctorow "Surveillance: You can Know Too Much" (17 June 2008) *Guardian* www.guardian.co.uk (accessed 25 June 2008).

802 See the discussion of privacy-enhancing technologies in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 151-156; Ann Cavoukian *Privacy and Radical Pragmatism: Change the Paradigm* (Office of the Information and Privacy Commissioner of Ontario, Toronto, 2008).

803 New Zealand Security Intelligence Service Act 1969; Government Communications Security Bureau Act 2003. For further information see www.nzsis.govt.nz and www.gcsb.govt.nz.

Law enforcement and regulation

8.40 Law enforcement agencies use a range of surveillance methods and devices in order to investigate offences. In 2007 the Law Commission released its report on the search and surveillance powers of law enforcement agencies.[804] It noted that surveillance was not regulated in any comprehensive way either by statute or by the common law. With regard to surveillance by law enforcement officers, the Commission recommended that there should be a single statutory framework for the use of audio, visual and tracking devices. Use of such devices by law enforcement officers should require authorisation by judicial warrant, except in urgent cases. The issue of surveillance by private individuals was outside the scope of the *Search and Surveillance Powers* report, and the Commission noted that this issue should be considered as part of a larger review of privacy protection in New Zealand.[805]

8.41 The Commission's recommendations concerning the search and surveillance powers of law enforcement agencies are proposed to be implemented by the Search and Surveillance Powers Bill 2008. The Bill provides that law enforcement officers must, in most circumstances, obtain a surveillance device warrant for the use of interception or tracking devices, and for the use of visual surveillance devices to observe or record private activity in a private building, or in the curtilage of a private building if the surveillance is prolonged.[806]

8.42 The Bill would only cover surveillance carried out by law enforcement officers. It is possible that some agencies may exercise regulatory inspection powers by means of surveillance; if so, such surveillance would fall outside the coverage of the Bill. Local authorities also sometimes use surveillance in the enforcement of laws and bylaws. For example, residents could be videotaped breaching bylaws imposing water restrictions,[807] or audio surveillance could be used to gather evidence about barking dogs pursuant to the Dog Control Act 1996.[808] Local authorities are also responsible for some environmental and traffic enforcement and for public CCTV cameras, which are discussed further below. Schools are another type of public authority that may use surveillance both for internal disciplinary purposes and to ensure compliance with statutes and regulations. Overseas, CCTV cameras, tracking devices and other forms of surveillance have been used in schools, and in New Zealand it is reported that some schools have hired private investigators to find out whether students are really living within the school zone.[809]

804 New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007). Chapter 11 of this report deals with interception and surveillance.

805 New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007) 327, 422-423.

806 Search and Surveillance Powers Bill 2008, no 300-1, cls 44-69 (see especially cls 44-46).

807 See *Woman Taped Watering Her Garden Received an Infringement Notice* [1999] NZPrivCmr 12 – Case Note 15052. Note, however, that this particular complaint related to taping on behalf of a media organisation, although at the invitation of the local authority, and that the taping was of the issuing of the infringement notice, rather than of the breach of the water restrictions itself.

808 *Stevenson v Hastings District Council* (14 March 2006) Human Rights Review Tribunal 7/06.

809 Urmee Khan "Teachers Fear Hidden CCTV Cameras in Schools" (17 August 2008) *Telegraph* www.telegraph.co.uk (accessed 20 October 2008); "Truants to be Tracked by GPS Anklets" (23 August 2008) www.msnbc.msn.com (accessed 20 October 2008); Mary Jane Boland "In the Zone" (30 August 2008) *The Listener* New Zealand 27, 28.

8.43 The use of surveillance powers by local authorities in the United Kingdom has been the subject of considerable controversy, with claims that the powers exercised have sometimes been disproportionate to the seriousness of the alleged offences which were being investigated.[810] There is currently no statutory provision for surveillance by local authorities in New Zealand, and the Search and Surveillance Powers Bill will cover local authorities only to a limited degree.

8.44 Although the use of surveillance in law enforcement investigations has already been considered by the Commission and is covered by the Search and Surveillance Powers Bill, it is still relevant to this Review. Consideration will need to be given to how any new regime for controlling surveillance outside the law enforcement context will interact with the law enforcement surveillance regime. There may also be some surveillance activities of regulatory agencies and local authorities that fall outside the law enforcement regime, but would be covered by a wider regime.

8.45 In addition, the Police and other law enforcement agencies may make use of information obtained through surveillance carried out by other individuals or agencies. For example, Police use images from CCTV cameras operated by local authorities or private businesses. In New South Wales, Police have launched a register of CCTV cameras, calling on businesses with such cameras to provide their details so that Police can more easily obtain footage. It is also reported that NSW Police are working on a system by which private citizens with video and photographic evidence of crimes (especially from cellphone cameras) could securely upload that footage via the internet to law enforcement agencies.[811] Both the benefits and the risks of the potential use by law enforcement of information obtained by others through surveillance need to be borne in mind in designing any new surveillance regime.

810 See for example "Spy Law 'Used in Dog Fouling War'" (27 April 2008) http://news.bbc.co.uk (accessed 12 May 2008); Richard Ford "Do we Really Need to use these Powers to Tackle Dog Fouling?" (31 May 2008) *The Times* www.timesonline.co.uk (accessed 3 June 2008); Alexi Mostrous "Terror Law Turns Thousands of Council Officials into Spies" (31 May 2008) *The Times* www.timesonline.co.uk (accessed 3 June 2008); Lee Glendinning "Councils Admit Using Information Laws to Monitor Residents" (6 June 2008) *Guardian* www.guardian.co.uk (accessed 6 June 2008); "Councils Warned Over Spying Laws" (23 June 2008) http://news.bbc.co.uk (accessed 24 June 2008); Chris Hastings "Anti-Terrorism Laws Used to Spy on Noisy Children" (6 September 2008) *Telegraph* www.telegraph.co.uk (accessed 8 September 2008). For a contrary view see Hugo Rifkind "Big Brother Only Wants to Help You" (21 November 2008) *The Times* www.timesonline.co.uk (accessed 12 December 2008). It should be noted that local authorities in the UK exercise a number of functions that in New Zealand are the province of central government. The legal framework in the UK is also different in that local council officials can be authorised to conduct some types of surveillance under the Regulation of Investigatory Powers Act 2000.

811 Josephine Asher "Police's CCTV Plan 'Violates Privacy Rights'" (18 February 2008) http://newsninemsn.com.au (accessed 27 June 2008); Marcus Brown "NSW Police Ask Public to be Cameraphone Cops" (26 March 2008) www.zdnet.com.au (accessed 31 March 2008).

Environmental and road traffic regulation

8.46 Environmental and road traffic regulation are two areas in which surveillance may be used increasingly in future. As New Zealanders become more concerned about issues such as climate change, energy efficiency, and waste disposal and recycling, there is potential for surveillance to be used more often in detecting whether or not individuals or companies are acting in an environmentally-responsible manner.[812]

8.47 Surveillance of vehicles on the roads is not new, but is likely to take different forms in future due to new and cheaper technologies, and also to concerns about the environment, crime and security. As Peter King writes: "Increasingly, our view of our cars as private space will be challenged by more revealing surveillance technology – some of it put up by roading authorities, some by retailers and some built into the very cars we drive."[813] In addition to existing speed cameras, New Zealand Police are now trialling automatic number-plate recognition (ANPR) cameras for identifying "vehicles of interest", and cameras at traffic lights to assist with prosecution of red light violations. The New Zealand Transport Agency does not provide direct video feeds to Police, in contrast to the Highway Agency in the United Kingdom.[814] In Australia there is a proposal for traffic cameras equipped with ANPR to be linked into a national network to assist with tracking of criminals.[815] Such a network will soon be fully operational in the United Kingdom, where data from ANPR cameras is retained for five years.[816]

8.48 Surveillance will probably also be used increasingly as part of strategies to deal with traffic congestion. For example, councils in Auckland photograph or videotape vehicles as part of the policing of transit lanes.[817] In future it is likely that some forms of road pricing (charging drivers based on the extent of their usage of roads) will be used to reduce congestion and encourage use of public transport, as well as to raise revenue. While road tolling is not a new idea, technologies such as ANPR or GPS can now be used to track vehicles for the

812 In the United Kingdom, it has been proposed by an advisory body that residents of planned "eco towns" should be monitored to ensure that their ecological footprints are within intended limits: Robert Booth "Eco Town Dwellers May be Monitored for Green Habits" (26 September 2008) *Guardian* www.guardian.co.uk (accessed 10 October 2008). Another example is the microchipping of rubbish and recycling bins in order to track the amount of waste being thrown out or recycled by households: Jano Gibson "Tracking Device on Bins Ensures Residents Chip In" (14 April 2008) *Sydney Morning Herald* www.smh.com.au (accessed 17 April 2008); Steve Doughty and Lucy Ballinger "Watched While You Throw: One in Five Wheelie Bins Microchipped as Councils Prepare for Bin Taxes" (31 May 2008) *Daily Mail* www.dailymail.co.uk (accessed 29 June 2008); Matthew Weaver "Microchip Bin Tax Scheme to Go Ahead Despite Failures" *Guardian* www.guardian.co.uk (accessed 29 June 2008).

813 Peter King "Eye Spy" (Winter 2008) *AA Directions* 34.

814 Peter King "Eye Spy" (Winter 2008) *AA Directions* 34-35. However, information from NZTA cameras may be passed on to Police: see Lincoln Tan "Transit Cameras Constantly on Patrol" (10 July 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 10 July 2008).

815 Mark Dunn "Privacy Worries Over Road Cameras Plan" (31 January 2008) *Herald Sun* Melbourne www.news.com.au (accessed 1 February 2008); Karen Dearne "Privacy Concerns on Speed Cameras" (23 September 2008) *The Australian* www.australianit.news.com.au (accessed 24 September 2008).

816 Paul Lewis "Fears Over Privacy as Police Expand Surveillance Project" (15 September 2008) *Guardian* www.guardian.co.uk (accessed 20 October 2008).

817 Wayne Thompson "Transit Lane Chancers a Pack of Dummies" (12 June 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 12 June 2008).

purpose of charging tolls.[818] The newly-opened Northern Gateway Toll Road, north of Auckland, uses ANPR for electronic toll collection.[819] In accordance with the Privacy Act and the provisions of the Land Transport Management Act 2003 relating to road tolling,[820] the New Zealand Transport Agency states that information collected through road tolling will be used only for purposes relating to the collection of tolls.

Security

8.49 Many uses of surveillance, including its use in law enforcement, are related to the protection of people's safety and security. The most obvious example is the use of CCTV cameras, but there are also other ways in which surveillance can be used for security. For example, biometric identification can be used for secure access to premises or computers; or tracking devices could be used to determine the location of people who may constitute a danger to others (such as certain categories of offenders released into the community, or accused persons released on bail) or to themselves (such as dementia patients).[821]

8.50 For many people, the use of CCTV cameras for security purposes has become synonymous with surveillance. CCTV is used to monitor and record activity in a particular area, with the aim of deterring crime and antisocial behaviour, as well as detecting and providing evidence of any offences that may take place. While some cameras are fixed, "pan, tilt and zoom" cameras can track and focus in on particular individuals or incidents. Cameras may be monitored continually by an operator (although this is unlikely in most cases), monitored some of the time, or used only to record. In most cases the cameras will record continually, with footage being kept for a limited period of time.

8.51 CCTV is widely used both by public authorities and by private businesses, although there are no figures on the number of such cameras in use in New Zealand. Local councils are increasingly using CCTV as part of their strategies for promoting safety and security. In some cases these cameras are directly monitored by Police, in others they are monitored by Council staff, contractors or volunteers, with information being passed on to the Police as required. For example, there are more than 50 public surveillance cameras in Auckland's central business district, covering most parts of the city centre. These cameras are monitored by non-sworn staff in the downtown Police station, and can zoom in close enough to read car registrations and facial expressions. However, Police are concerned that their deterrent value is undermined by a lack of public awareness of the cameras' presence.

---

818 Stephen Graham with David Murakami Wood "Expert Report: Infrastructure and Built Environment" 7-8 in Appendix 4 to Surveillance Studies Network *A Report on the Surveillance Society* (report for the UK Information Commissioner, 2006); Institution of Professional Engineers New Zealand *Transport: Engineering the Way Forward* (Wellington, 2008) 20; Kim Murphy "Oregon Mulls Tax on Miles Driven" (5 January 2009) *Chicago Tribune* www.chicagotribune.com (accessed 6 January 2009).

819 See www.tollroad.govt.nz.

820 Land Transport Management Act 2003, s 50. Note that s 50(4) provides that disclosure of personal information collected is allowed on any of the grounds set out in information privacy principle 11 in the Privacy Act.

821 Craig Offman "You are Tagged" (3 December 2007) *National Post* Canada www.nationalpost.com (accessed 5 December 2007); Brian Brady "Prisoners 'To be Chipped Like Dogs'" (13 January 2008) *Independent* www.independent.co.uk (accessed 16 January 2008); "Judge Calls for Electronic Tags for Some Youth" (20 October 2008) www.radionz.co.nz (accessed 21 October 2008).

They are looking at measures such as newspaper advertisements, more prominent signage, and even flashing blue lights above the cameras so that people will be more aware that the cameras are there.[822]

8.52 There appears to be a popular assumption that CCTV cameras are effective tools in fighting crime, and consequently they appear to make people feel safer. This perception is backed up by reports of particular cases in which CCTV footage has been important in detecting and prosecuting crimes.[823] The Ministry of Justice's *National Guidelines for Crime Prevention Through Environmental Design in New Zealand* emphasise the importance of "informal surveillance" by members of the public through the creation of public spaces with clear sightlines and good lighting to ensure maximum visibility. However, they also note that CCTV can play a role in preventing and detecting crime if it is implemented in association with a wider range of crime prevention measures.[824]

8.53 The effectiveness of CCTV surveillance in preventing, detecting and prosecuting crime is the subject of considerable debate. We are not aware of any detailed New Zealand studies on this question,[825] but evidence from overseas provides a somewhat mixed picture.[826] In particular, there appears to be little evidence that CCTV cameras deter crime, except in semi-open spaces such as car parks. They appear to be more useful in detecting crime and providing evidence for prosecution of crime. To the extent that they can assist in reducing crime, CCTV cameras appear to be more effective in relation to premeditated and property crime than violent crime or public disorder. Assessing the value of CCTV in responding to crime is beyond the scope of this issues paper, but we note the need for further research on the subject in New Zealand.

822 Elizabeth Binning "Cameras Watch the City Almost Undetected" (30 June 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 30 June 2008); see also Bernard Orsman, Louisa Cleave and Martin Johnston "'Eyes' Monitor Every Movement" (30 July 2005) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 2 November 2007).

823 See for example Lucy Vickers "Shocking Images Show Value of CCTV" (16 May 2008) *North Shore Times* Auckland www.stuff.co.nz (accessed 16 May 2008); "Catching 'Muppets' on Camera" (18 June 2008) *Capital Times* Wellington 2; Elizabeth Binning "Cameras Watch the City Almost Undetected" (30 June 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 30 June 2008).

824 Ministry of Justice *National Guidelines for Crime Prevention Through Environmental Design in New Zealand. Part 1: Seven Qualities of Safer Places* (Wellington, 2005).

825 The Manukau City Council has attempted to assess the effectiveness of its CCTV systems, but the results are inconclusive: Manukau City Council *Closed Circuit Television Camera (CCTV) Strategy: Final for Adoption* (April 2006) appendix 3.

826 For some reviews of overseas research on the effectiveness of CCTV, see Dean Wilson and Adam Sutton "Watched Over or Over-Watched? Open Street CCTV in Australia" (2004) 37 Australian and New Zealand Journal of Criminology 211; Martin Gill and Angela Spriggs *Assessing the Impact of CCTV* (Home Office Research, Development and Statistics Directorate, London, 2005); Nigel Brew "An Overview of the Effectiveness of Closed Circuit Television (CCTV) Surveillance" (Parliament of Australia, Parliamentary Library, Research Note No 14 2005-06, 28 October 2005) www.aph.gov.au (accessed 20 October 2008); Jerry Ratcliffe *Video Surveillance of Public Places* (United States Department of Justice, Office of Community Oriented Police Services, Washington, DC, 2006); John Honovich "Video Surveillance Review: Is Public CCTV Effective?" (8 July 2008) http://ipvideomarket.info (accessed 8 August 2008); Surveillance Camera Awareness Network *A Report on Camera Surveillance in Canada: Part One* (The Surveillance Project, Queen's University, Kingston, Ontario, Canada, 2009).

Commercial

8.54 We have already referred to the use of surveillance by private businesses for security purposes. The use of surveillance in the workplace is discussed in chapter 12. We also discuss in chapter 12 the role of private investigators, who are sometimes employed by businesses (for example, to investigate insurance fraud). In addition, surveillance could be used by companies to gather intelligence about commercial competitors, or about protesters or others who may be seen as posing a threat to a company.

8.55 Another potential use of surveillance in the commercial arena is for gathering information about customer preferences and activity patterns.[827] We discussed in *Privacy: Concepts and Issues* covert tracking by companies of the online activity of internet users.[828] Other examples include:

- Tracking customer movements (for example, which shops they visit, and for how long) by monitoring their mobile phone signals.[829]
- Equipping billboards with cameras that analyse facial features of passers-by to determine their gender, race and approximate age, and record how long they looked at the billboard, in order to target digital advertising.[830]
- Gaze-tracking technology that monitors eyeball movements and can determine which products or displays customers are looking at.[831]

8.56 Although not yet in general commercial use in New Zealand, RFID technology is likely to enable businesses to collect even more consumer information in future. The RFID tag on a product links to a database containing information about the product or its purchase, and can also provide location information.[832] A key difference between RFID tags and bar codes is the potential for RFID tags to continue providing information to businesses both before and long after the moment of purchase, if they are not deactivated. In retail environments, RFID scanners could potentially track people through a store by the RFID tags they are wearing, link this to their personal information when they use their credit card or store card, and monitor their in-store behaviour.[833] The ability of RFID scanners to collect data from tags once a consumer has left a store or

827 See Stephen Baker *The Numerati* (Houghton Mifflin, Boston, 2008) ch 2; "The Way the Brain Buys" (20 December 2008) *The Economist* 105.

828 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 128-130.

829 Jonathan Richards "Shops Track Customers Via Mobile Phone" (16 May 2008) *The Times* www.timesonline.co.uk (accessed 22 May 2008).

830 Stephanie Clifford "Billboards That Look Back" (31 May 2008) *New York Times* www.nytimes.com (accessed 4 June 2008); Dinesh Ramde "High Tech Ads Watch You Watching Them" (2 February 2009) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 3 February 2009).

831 Brad Reed "Study: Surveillance Software Revenue to Quadruple by 2013" (2 June 2008) *CIO* www.cio.com (accessed 4 June 2008).

832 For an overview of the development of RFID, see Katherine Albrecht, "RFID tag – You're it" (September 2008) *Scientific American* 72.

833 Katherine Albrecht, "RFID Tag – You're it" (September 2008) *Scientific American* 75. Rachel Bowie "Day of the RFIDs" (September 2007) *Consumer* New Zealand 40, cites a US trial of RFID-tagged Max Factor lipsticks that triggered a webcam when picked up from the shelf to study the behaviour of consumers.

moved beyond the readers' range is currently limited,[834] but the tracking potential of RFID technology is projected to improve as it develops and converges with other technologies.[835]

8.57 It is important to emphasise that some of these customer-tracking technologies are still some years away from being in widespread use,[836] and we are not aware of examples of their use in New Zealand. It should also be noted that in many cases they track people anonymously or without retaining personal information. Nonetheless, they have the capacity to be used for monitoring individual behaviour. Some people may also feel that such monitoring is an intrusion, even if it is not used to monitor them as individuals.

Domestic

8.58 Surveillance can be used by private individuals in and around their homes, and in relation to their domestic affairs. Domestic surveillance is becoming easier as surveillance devices are becoming smaller, cheaper and integrated with other technologies, such as cellphones. Such surveillance can take many forms, including:

- surveillance cameras for security purposes;[837]
- video surveillance of neighbours, particularly in the context of disputes between neighbours;[838]
- surveillance of current or former partners for purposes such as detecting infidelity or providing evidence for custody disputes;[839]
- surveillance of children to detect drug use or other activity that parents may be concerned about;[840]
- camera surveillance of nannies or other domestic workers;[841] and
- self-surveillance by live internet broadcasts of individuals' lives via webcam (which may also involve broadcasting their interactions with other people).[842]

834 Privacy International "Radio Frequency Identification (RFID)" (18 December 2007) www.privacyinternational.org (accessed 31 October 2008).

835 For example, the combination of RFID with Wi-Fi (wireless) technology could increase the distance from which tags can be scanned, even raising the possibility of remote tracking: "Wi-fi and RFID Used for Tracking" (25 May 2007) http://news.bbc.co.uk (accessed 1 December 2008).

836 Ben Woodhead "Shopper Tracking Face Privacy Concerns" (4 March 2008) *Australian* www.australianit.news.com.au (accessed 5 March 2008).

837 For examples of security camera systems that can be linked to a home computer and viewed via the internet or cellphone, see Kirk Steer "Do-it-yourself Surveillance Protects Home or Business" (28 August 2007) *New Zealand PC World* www.pcworld.co.nz (accessed 19 June 2008).

838 *Neighbours Camera Aimed Directly Into the Complainant's Living Area* [1994] NZPrivCmr – Case Note 1635; Alice Hudson "Big Sister Isn't Watching You" (16 December 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 17 December 2007). Note however that in both of these cases the cameras turned out to be fakes.

839 Brad Stone "Tell-All PCs and Phones Transforming Divorce" (15 September 2007) *New York Times* www.nytimes.com (accessed 19 September 2007); Leigh van der Stoep "Spying on Your Partner Just Got Easier" and "Why Spying on Spouses may be a Really Bad Call" (21 and 28 September 2008) *Sunday Star-Times* www.stuff.co.nz (accessed 26 and 29 September 2008).

840 Catherine Woulfe "Spyware Sales on the Increase" (27 April 2008) *Sunday Star-Times*.

841 Amy Reiter "Putting Mary Poppins Under Surveillance" (17 July 2003) www.salon.com (accessed 1 July 2008).

842 Hal Niedzviecki "The Spy Who Blogged Me: How We Learned to Stop Worrying and Love Surveillance" (16 June 2008) *The Walrus* Canada www.walrusmagazine.com (accessed 17 June 2008); Stephen T Watson "Video Technology Creates a Few Very Public Lives" (29 December 2008) *Buffalo News* Buffalo (NY) www.buffalonews.com (accessed 5 January 2009).

8.59 Domestic surveillance is covered by the same existing laws as other forms of surveillance, but there is an important exception in section 56 of the Privacy Act 1993. This section provides that the information privacy principles do not apply to the collection and holding of personal information by an individual "solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs". Consequently, no remedies may be available under the Act in some cases of domestic surveillance.

Research

8.60 Research in the social sciences, psychology, medicine and other fields will often involve monitoring of living human subjects. Such monitoring is a form of surveillance, but is not usually considered problematic so long as the subjects have consented. Codes of ethics of universities, funding bodies and other organisations in New Zealand generally require that participants in research involving human subjects must give informed consent to their participation. However, there will be cases in which it is not practical to obtain consent, or in which informing the subjects would distort the results.[843]

Conclusion

8.61 In this section we have described many different ways in which surveillance is used, and some additional uses will be discussed in chapter 12. Although these uses are quite diverse, all involve intentional monitoring or observation using devices. There is also considerable cross-over between the different forms of surveillance we have outlined: for example, Police and the media may make use of footage from public and private security cameras. Many of the uses of surveillance would be widely viewed as beneficial, particularly in deterring and detecting crime and serious wrongdoing. However, surveillance can also have negative effects, which we will now discuss.

843 For overseas examples see Seth Borenstein "Study Secretly Tracks Cellphone Users" (4 June 2008) *Globe and Mail* Toronto www.theglobeandmail.com (accessed 6 June 2008); John Schwartz "Cellphone Tracking Study Shows We're Creatures of Habit" (5 June 2008) *New York Times* www.nytimes.com (accessed 6 June 2008); Vassilis Kostakos "Bluetooth Monitoring can Bring Many Benefits" (21 July 2008) http://blogs.guardian.co.uk (accessed 22 July 2008).

Q32 Which of the following types of surveillance are you particularly concerned about? What are your main concerns about these types of surveillance? Which of these types of surveillance do you consider particularly beneficial, and why? (Note that surveillance for intelligence and law enforcement purposes is largely outside the scope of this Review, and that workplace, private investigator and media surveillance are discussed in chapter 12.)

- Regulatory (including local government, environmental and traffic regulation)
- Security (including CCTV)
- Commercial
- Domestic
- Research
- Workplace
- Private Investigator
- Media
- Other

NEGATIVE EFFECTS OF SURVEILLANCE

8.62 In this section we consider some of the possible harms to individuals and society from surveillance, including threats to privacy but also other types of harm. Both overt and covert surveillance can have negative effects, although the nature of the effects may differ between these two forms of surveillance.[844]

Civil liberties and the chilling effect of being watched

8.63 Surveillance can be used to deter behaviour that is considered criminal or anti-social, but there is a danger that excessive surveillance could also deter behaviour that is eccentric, spontaneous or subject to social or political disapproval. It could, for example, deter legitimate protest and political activism. On the other hand, people do not know when they are the subjects of covert surveillance, although there could be a chilling effect if they have reason to suspect they might be, or find out later that they have been, put under surveillance. In the case of overt video surveillance, it appears that many people are not conscious of the cameras' presence, so it is perhaps questionable whether their behaviour is in fact affected. It may be, as Derek Lai suggests, that "Mere 'watching' by itself does not seem to account for a chilling effect. Rather, some type of negative consequence must attach to the 'watching' before the behaviour can be 'chilled'."[845]

844 For further discussion see New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC No 98, Sydney, 2001) 118-141; Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006) 38-48; Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta L Rev 43, 50-57.

845 Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta L Rev 43, 50.

Loss of anonymity

8.64 While it is perhaps less possible to be anonymous in New Zealand than in some larger societies, we still expect that most people will not know us or pay particular attention to us, even in public. By focusing on particular individuals, however, surveillance can undermine this expectation of anonymity. A snatch of conversation overheard on a public street will most likely mean nothing to a passer-by, but the systematic monitoring of that conversation by someone who has a particular interest in the participants is a quite different matter. In the latter case the participants are known to the observer (or the aim may be to discover their identities); their words may be subject to close scrutiny, and put together with other information known about them; and the monitoring of their conversations may lead to negative consequences for them.

Stress and emotional harm

8.65 Being the subject of surveillance can be stressful, particularly if it is prolonged and if it may result in adverse action being taken against those who are being monitored. There is evidence, for example, that workplace monitoring can be stressful for employees, although the effects of such surveillance depend on a range of factors.[846] Finding out that a person has been the subject of covert surveillance may also be stressful for that individual, and may lead to feelings of powerlessness, violation and insecurity. In addition, people may be distressed and embarrassed about what may have been revealed about them in the course of the surveillance.

Recording

8.66 Most forms of surveillance create a record of the activities and communications monitored. This can have a number of consequences:

- a permanent record of an event or communication can be created;
- the information gathered can be analysed in more detail than would be possible from casual observation, and can be combined with other information;
- information can be taken out of context; and
- information can be disseminated widely, to audiences other than those the subject intended to communicate with or be observed by.

With the exception of taking information out of context, these are some of the very features that make surveillance useful in gathering evidence of criminality or other serious wrongdoing, but they also create potential for abuse. The records obtained through surveillance can be used selectively, used for purposes such as blackmail and intimidation, or simply used for purposes that do not justify the level of intrusion involved.

846 Kirstie Ball "Expert Report: Workplace" 5-7 in Appendix 4 to Surveillance Studies Network *A Report on the Surveillance Society* (report for the UK Information Commissioner, 2006). See also Ben Farmer "More Employees Under Surveillance at Work" (9 January 2008) *Telegraph* www.telegraph.co.uk (accessed 2 July 2008); Nick Heath "'Big Brother IT' Fuels Workplace Stress" (8 January 2008) www.silicon.com (accessed 14 January 2008); "Surveillance Cameras at Work Are Stressful: SKorean Court" (9 April 2008) http://afp.google.com (accessed 2 July 2008).

Excessive collection of personal information

8.67 Mass surveillance, such as that conducted using CCTV cameras, will collect information about many people who have done nothing wrong and are of no immediate interest to those who are doing the monitoring. Targeted surveillance may also inadvertently collect information about people who are not the targets of surveillance, or may collect information about the targets that is of no relevance to the matter being investigated. Those who are the subjects of surveillance may also ultimately prove to be innocent. The capacity of modern digital technologies to collect, store and analyse information is enormous, and growing all the time. This means that a vast amount of personal information obtained through surveillance could, potentially, be stored for future use even if it is of no immediate interest. Controls on retention and use of personal information, like those in the Privacy Act 1993, are therefore vital.

Insecurity and loss of trust

8.68 Surveillance is often used for purposes connected to individual and public security, and to make people feel safer in their homes and communities. However, if the surveillance is felt to be inappropriately targeted at particular individuals or groups, excessive or disproportionate to its objectives, carried out for improper motives, or otherwise illegitimate or inappropriate, it can undermine trust in those undertaking the surveillance. It may also make those who have been the targets of surveillance, or who feel that they might be, feel more insecure. This is particularly true if the surveillance has been covert. With regard to overt, public surveillance systems such as CCTV cameras, it appears that these do make many people feel more secure. However, it can be argued that the proliferation of surveillance cameras may create a feeling of being under threat that is not justified by the actual level of threat from crime or disorder.

Use for questionable purposes

8.69 While voyeurism is rarely the primary purpose of surveillance, voyeuristic use can sometimes be made of surveillance systems set up for other purposes. There have been examples of CCTV cameras being used to track women, and zoom in on particular parts of their bodies. Footage from surveillance cameras may also be used for its entertainment or prurient value on internet sites such as YouTube, or in other media, without the subjects' permission.[847]

8.70 Another problem concerning the purposes for which surveillance is used is "function creep". Surveillance introduced for one purpose that has widespread support may subsequently be used for other purposes which have less justification or public support.

847 Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta L Rev 43, 55-56; Marina Hyde "This Surveillance Onslaught is Draconian and Creepy" (28 June 2008) *Guardian* www.guardian.co.uk (accessed 29 June 2008); "Web Intimacy Video Spurs Concern about Management, Privacy" (20 January 2008) http://news.xinhuanet.com/english (accessed 22 January 2008); Claire Truscott "Couple Sue After Thousands See Film of Subway Kiss" (22 January 2008) *Guardian* www.guardian.co.uk (accessed 23 January 2008); American Civil Liberties Union "True Stories" at www.youarebeingwatched.us (accessed 15 January 2009).

Discrimination, profiling and misidentification

8.71 Any mass surveillance system is designed to discriminate in the sense of being used to draw distinctions between people: citizens or non-citizens, terrorists or non-terrorists, people who prefer Brand X or people who prefer Brand Y, and so on. Such forms of discrimination are inevitable and, in many cases, essential. Nonetheless, the use of surveillance for profiling and "social sorting" (the exercise of social control by categorising individuals based on certain characteristics) can raise serious concerns.[848] In particular, it raises the prospect of differential treatment of people based on characteristics over which they have no control, leading to the creation or entrenchment of inequalities. For example, there is evidence from overseas that those monitoring CCTV may tend to focus on people based on their race, age, and other aspects of their appearance.[849]

8.72 A related problem of sorting concerns the use of surveillance to identify individuals. There is always a danger of misidentification, which in some cases can lead to very serious consequences for the person concerned. An exaggerated faith in the capacity of new technologies to identify individuals can be dangerous, and special measures may be needed to address this.[850]

Desensitisation

8.73 There is a danger that, as surveillance becomes more widespread, individuals and society will become desensitised to it, treating it as simply a fact of life rather than something to be questioned. Overt surveillance devices may simply become "part of the furniture" that people take no account of. This possibility may run counter to the idea that surveillance has a chilling effect on behaviour and expression, although that effect could still operate subliminally. Moreover, people may still find to their cost that information obtained through surveillance can be unexpectedly used against them. A related danger is that, as technology develops and surveillance becomes more prevalent, there may be fewer and fewer circumstances in which society and the law consider that an individual has a reasonable expectation of privacy.

PUBLIC ATTITUDES

8.74 Anecdotal and research evidence from New Zealand and elsewhere suggests a low level of public concern about some forms of surveillance, and a significant level of support for CCTV in particular. It is clear, however, that attitudes vary depending on the particular form of surveillance, and also vary to some degree among different segments of the population.

848 On social sorting see David Lyon (ed) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (Routledge, London, 2003).

849 See for example Clive Norris and Gary Armstrong "CCTV and the Social Structuring of Surveillance" in Clive Norris and Dean Wilson (eds) *Surveillance, Crime and Social Control* (Ashgate Publishing Limited, Aldershot, 2006) 81; Ann Rudinow Sætnan, Heidi Mork Lomell and Carsten Wiecek "Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish Observations" (2004) 2 Surveillance & Society 396.

850 See for example Ruth Costigan "Identification from CCTV: The Risk of Injustice" [2007] Crim LR 591.

New Zealand

8.75 In New Zealand, opinion surveys conducted for the Office of the Privacy Commissioner show differing levels of concern about a number of activities that could be considered forms of surveillance. In the 2008 survey, 67 per cent of respondents were uncomfortable with internet search engines and social networking sites tracking their internet use and emails and delivering targeted advertising to them. With regard to other surveillance-like activities, 46 per cent were concerned about employer monitoring of emails and internet use; 35 per cent about the use of biometrics to identify people; and 27 per cent about video surveillance in public places. Māori were more likely to be concerned about some forms of surveillance than non-Māori: 43 per of Māori were concerned about biometrics, compared to 32 per cent of non-Māori, and Māori were also somewhat more likely to be concerned about video surveillance in public places (33 per cent of Māori, 25 per cent of non-Māori).[851]

8.76 Surveys conducted for the Broadcasting Standards Authority give some indication of attitudes to surveillance-like activities by the broadcast media. In a 1999 survey, a scenario was presented in which a member of the public is filmed, using a hidden camera, entering a strip club. This was considered unacceptable by 74 per cent of those taking part in the survey, and the filming of a politician in the same circumstances was considered unacceptable by 64 per cent.[852] Another survey in 2003 presented a number of scenarios relating to a New Zealand psychologist suspected of sexually harassing patients, who has refused all approaches from the media. Forty-two per cent of respondents considered it unacceptable to use a hidden microphone to tape the psychologist seeing a patient, while 46 per cent considered it unacceptable to use a hidden camera. Just under a quarter of respondents considered it acceptable, with most remaining respondents taking a middle-ground position.[853]

United Kingdom

8.77 More detailed research, both quantitative and qualitative, on attitudes to surveillance has been carried out in the United Kingdom. While the situations in the two countries are quite different in a number of respects, the British research may nonetheless be instructive for New Zealand.

851 Privacy Commissioner and UMR Research *Individual Privacy and Personal Information: Omnibus Results*, available at www.privacy.org.nz. The survey of 750 people (11 per cent Māori) aged 18 and over was carried out in July 2008. The 2006 Privacy Commissioner survey also asked about "Government interception of telephone calls or email", which 72 per cent of respondents were concerned about: see 2006 survey results summarised in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 116-117.

852 Gary Dickinson, Michael Hill and Wiebe Zwaga *Monitoring Community Attitudes in Changing Mediascapes* (Dunmore Press/Broadcasting Standards Authority, Palmerston North, 2000) 88. The survey of 1000 people aged 15 and over was carried out in March-April 1999.

853 Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press/Broadcasting Standards Authority, Wellington, 2004) 101. The survey of 1195 people aged 15 and over was conducted in February-March 2003.

8.78 A 2006 public opinion survey asked people about their attitudes to a range of surveillance activities.[854] It revealed a high level of support (between 85 and 97 per cent) for CCTV cameras in various types of public places. There were quite different results for other forms of surveillance. Photographing airline passengers was supported by 72 per cent, but only 45 per cent approved of fingerprinting airline passengers. Only half of those surveyed approved of speed cameras, 70 per cent disapproved of using the chips in identity cards to track the movement of every individual possessing such cards, and 79 per cent disapproved of using high-powered microphones to listen in on conversations in the street. Gender had a more significant effect on attitudes than either age or social class, with women more likely than men to approve of surveillance, sometimes quite significantly so. For example, 57 per cent of women and only 42 per cent of men approved of speed cameras, while 51 per cent of women supported fingerprinting airline passengers, compared to only 40 per cent of men.

8.79 Qualitative research carried out in 2007 on behalf of the UK Information Commissioner's Office helps to add context to the quantitative data.[855] On the whole, people were not particularly worried about surveillance, and were more concerned about identity fraud and the collection and use of data by commercial organisations (which they did not see as surveillance). There was a high level of support for CCTV, which was believed to assist in reducing crime and apprehending criminals, and which made people feel safer. Media stories about the use of CCTV to catch criminals reinforced these views.

CONCLUSION

8.80 This chapter has established that surveillance has many uses, at least some of which are socially beneficial, and that public opinion appears to be relatively unconcerned about or supportive of some forms of surveillance. We do not believe, therefore, that surveillance should be banned outright, or that its use should be restricted entirely to law enforcement agencies. However, surveillance has significant dangers if it is unconstrained, and there is evidence of public concern about some types of surveillance. For these reasons, we believe that surveillance should be regulated to some degree, a conclusion that is supported by the current controls on surveillance, patchy though they may be. The questions, then, are: what forms of surveillance should be controlled, and in what ways should they be controlled? This is the issue to which we will return when we consider law reform options in chapter 10.

854 YouGov/Daily Telegraph survey of 1979 people aged 18 and over, carried out in November 2006, available at www.yougov.com.

855 Oliver Murphy *A Surveillance Society: Qualitative Research Report* (Diagnostics Social & Market Research, report prepared for the United Kingdom Information Commissioner's Office, 2007). The study was conducted with 12 discussion groups, each with six respondents, in a range of UK locations.

Chapter 9

Surveillance: the existing law

9.1 In this chapter we examine the law that applies to the use of surveillance devices, including visual surveillance devices (such as binoculars, cameras and video recorders); listening and interception devices (such as bugs, tape recorders and telephone interceptors); locating and tracking devices (such as GPS-enabled devices and cell phones); and data surveillance devices (such as spy software and keystroke loggers). In some cases, surveillance is carried out by co-opting a device used or carried by the target (for example, converting a cellphone into an interception or tracking device).

9.2 This chapter outlines the criminal and civil law, as well as regulatory controls, that currently apply to surveillance. We then give examples which may suggest the inadequacies of the existing laws.

SURVEILLANCE AND THE CRIMINAL LAW

Watching and visual recording

9.3 The current law criminalises certain uses of visual surveillance devices including:

- Intimate covert visual recording: that is, surreptitiously filming or photographing people without their consent in places where they reasonably expect to be private, while they are in a state of undress or engaged in private sexual activity or toileting; or surreptitiously filming or photographing people's private body parts from under their clothing (up-skirt filming).[856]
- The making of a publication such as photograph, picture, film or computer file that is "objectionable".[857]

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

857 Films, Videos and Publications Act 1993, s 123. A publication is objectionable if it describes, depicts, expresses or otherwise deals with matters such as sex, horror, crime, cruelty or violence in such a manner that the availability of the publication is likely to be injurious to the public good: s 3(1). Further offences include copying, importing, supplying, distributing, possessing, displaying and advertising an objectionable publication: see ss 123(1), 124, 129, 131, 131A, 132.

- Taking or using any photograph, videotape recording or cinematographic film of a person, without the person's consent, in connection with the business of a private investigator.[858] This provision may also cover the installation of hidden cameras by private investigators, even if they are operated by someone else, as the offence applies both to the taking of pictures or films and causing pictures or films to be taken.

9.4 Other relevant offences that can extend to the use of visual surveillance devices include:

- peeping and peering into a dwelling-house at night, without reasonable excuse;[859]
- offensive behaviour in a public place;[860]
- intimidation by watching or loitering near a place where a person lives, works, carries on business or happens to be, with intent to frighten or intimidate;[861] and
- harassment by watching or loitering near a person's place of residence, business, employment or any other place a person frequents, or following a person (on at least two occasions within 12 months) if it causes the person to reasonably fear for his or her safety.[862]

Visual surveillance in public places

9.5 Generally, photographing or filming people in public places is not restricted by the criminal law. However, there are exceptions, as the offences listed in paragraphs 9.3 and 9.4 show. Examples of visual surveillance in a public place that could constitute an offence include photography by a private investigator, "up-skirt" filming, and conduct amounting to intimidation or harassment. In addition, two cases involving the same defendant have considered whether taking surreptitious photographs of people in a public places can amount to offensive behaviour under section 4 of the Summary Offences Act.[863]

9.6 In the first case,[864] a police constable who had been tipped off by a photo developer discovered a man taking photographs of teenage schoolgirls through a gap in the curtains of his bus parked near the entrance to the girls' school. On investigation, the bus was found to contain two cameras with large lenses, photograph albums containing numerous photographs of young girls and numerous rolls of undeveloped film. Once developed, the films were found to contain further photographs of girls in the vicinity of the school. While they were unaware at the time that they were being photographed, on being interviewed the girls reported feeling upset, offended and concerned about the photographs being taken near their school. The school principal's view was that the images were disturbing, upsetting and offensive. She had seen the bus parked near the school on many occasions.

858 Private Investigators and Security Guards Act 1974, s 52.

859 Summary Offences Act 1981, s 30.

860 Summary Offences Act 1981, s 4.

861 Summary Offences Act 1981, s 21.

862 Harassment Act 1997, ss 4 and 8.

863 See Paul Roth "Unlawful Photography in Public Places: the New Zealand Position" [2006] PLPR 2.

864 *R v Rowe* [2005] 2 NZLR 833 (CA).

9.7 The man was prosecuted for offensive behaviour in a public place under section 4 of the Summary Offences Act 1981. There were some difficulties with fitting the covert surveillance within the scope of the charge. As the photography was surreptitious, it arguably did not have the necessary potential to cause serious offence because it was not observable by anyone in the street, other than the police constable who discovered it. The Court of Appeal found that the case was near to the margin. The conduct had to speak for itself and could not take into account the pattern of behaviour such as the photograph albums and the other rolls of film that were found. But one factor taken into account was the lack of a legitimate purpose.

9.8 Two Judges (the majority) considered that the photography did have the necessary tendency to seriously offend "right-thinking members of the community" and that it warranted the intervention of the criminal law even without proof that any offence was actually taken at the time of the conduct. The minority Judge considered that the photography did not meet the test for offensive behaviour, noting that while offence may be caused if the photographs were used for a sinister purpose, it would be the use which caused offence, not the taking of the photographs.

9.9 In the second case,[865] the man was observed by a librarian in a university library furtively taking photographs. On being approached by the university constable, his digital camera and laptop were found to contain a number of photographs of female occupants of the library seated at their desks. The women were unaware that they had been photographed but on learning of the photography, they reported feelings of anxiety and being uncomfortable about the photographs being taken for some purpose they did not know about.

9.10 The man was again charged with offensive behaviour in a public place. He was convicted in the District Court, but succeeded on appeal to the High Court in having the conviction quashed. In the Judge's view, the case was more marginal than the circumstances in the first case. Applying the "reasonable observer" test, the behaviour observed would not cause a reasonable observer to be offended. The test required an assessment of the effect of the behaviour on those who observed it (the librarian and the university constable), and did not allow account to be taken of the privacy intrusion on the women who were the subject of the photography because they had not observed it (due to its surreptitious nature).

9.11 Whether the summary offence of offensive behaviour in a public place applies to overt, as opposed to covert, visual surveillance, will depend on the circumstances of any particular case.[866]

865 *Rowe v Police* (12 December 2005) HC DN CRI 412-000051, John Hansen J. For a similar case in the United States see Debra Friedman "Man Faces New Charges in Taping" (9 October 2008) *Greenwitch Time* www.greenwitchtime.com (accessed 13 October 2008) where a man pleaded guilty to breach of the peace for videotaping patrons at a public library.

866 See for example the case of a man photographing women bathing topless at a Sydney beach who was prosecuted for offensive behaviour, cited in Christa Ludlow "'The Gentlest of Predations: Photography and Privacy Law" (2006) 10 Law Text Culture 135.

CCTV and the criminal law

9.12 The use of CCTV is unlikely to invoke any of the criminal offence provisions that apply to visual surveillance. For example, the summary offence of peeping and peering has a defence of reasonable excuse. The use of CCTV for public purposes such as crime prevention and security would likely provide a reasonable excuse, provided operating procedures were followed. However, the use of CCTV cameras that have an audio function to listen to and intercept a private conversation may breach the interception offence, and the use of CCTV by private investigators is restricted.[867]

Listening and interception

9.13 The use of devices for audio surveillance and interception is controlled under Part 9A of the Crimes Act 1961.[868] Previously the offence dealt with the interception of private conversations by listening devices, consistently with the form of comparable offences enacted in various Australian states.[869] In New Zealand, however, the scope of the offence was broadened to control the interception of written and electronic communications (including email and text messages) by updating legislation in 2003.[870]

9.14 The primary offence is the intentional interception[871] of a private communication by means of an interception device.[872] Key factors are whether an interception device[873] was used, whether the target communication was a "private communication,"[874] and whether any of the listed exceptions apply.

867 Private Investigators and Security Guards Act 1974, s 52.

868 There is also an interception warrant regime in relation to drug dealing offences in the Misuse of Drugs Amendment Act 1978, Part 2.

869 Surveillance Devices Act 1998 (WA), s 5(1); Surveillance Devices Act 1999 (Vic), s 6(1); Surveillance Devices Act 2007 (NSW), s 7; Surveillance Devices Act 2007 (NT), s 11; Listening and Surveillance Devices Act (SA), s 4; Invasion of Privacy Act 1971 (Qld), s 42.

870 Crimes Amendment Act 2003, s 9; Hon Bruce Robertson (ed) *Adams on Criminal Law* (loose leaf, Brookers, Wellington, Crimes Act, 1992) para CA216B.01 (last updated 19 October 2007). For discussion of the legislative history, see *Moreton v Police* [2002] 2 NZLR 234, paras 15-19 (HC) William Young J.

871 "Intercept," in relation to a private communication, includes hear, listen to, record, monitor, acquire, or receive the communication either (a) while it is taking place; or (b) while it is in transit: Crimes Act 1961, s 216A(1). The offence does not cover the interception of stored communications such as the copying of stored emails, the surreptitious recording of answer-phone messages, or the interception of email messages through the use of keystroke loggers before the messages are sent.

872 Crimes Act 1961, s 216B(1).

873 "Interception device" is defined as any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication, other than a hearing aid or any exempted device: Crimes Act 1961, s 216A(1).

874 "Private communication" is defined in the Crimes Act 1961, s 216A(1) as:

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

(b) does not include such a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so.

9.15 There are a number of exceptions to the interception offence that permit law enforcement officers to intercept private communications where authorised by an interception warrant or in an emergency, and permit the intelligence services to intercept private communications in accordance with their statutes.[875] There are also exceptions for the monitoring of prisoner calls, and for interception carried out in conjunction with the maintenance of the internet or other communication services.[876]

9.16 An important exception to the interception offence is participant monitoring.[877] Participant monitoring takes two forms:

- the recording of one's own communications with another person or persons, without their knowledge or consent (principal party recording);
- facilitating or permitting the interception of one's own communications by outsiders to the communication without the knowledge or consent of other participants (authorised outsider monitoring).[878]

Locating and tracking

9.17 There is no specific offence against the covert use of location and tracking devices. The law restricts the unauthorised entry onto premises (tort of trespass to land) and the interference with a person's property (tort of trespass to goods). These torts limit the installation of tracking devices to some extent, but they are civil remedies that target interferences with property rather than privacy and do not involve prosecution of the person carrying out the tracking.

9.18 The Harassment Act applies to some locating and tracking activities such as watching and following another person,[879] but it is not clear whether the Act could apply to locating and tracking someone remotely through the covert use of devices.

9.19 The use of tracking devices by law enforcement officers is controlled through the tracking devices regime which allows for the use of tracking devices by police and Customs officers under a warrant and in emergency situations.[880] However, there is no corresponding offence provision.[881] At the time the tracking device regime was introduced, the Privacy Commissioner submitted that a tracking offence should be part of the regime; however, the Select Committee felt that a tracking offence was not necessary at that time.

875 Crimes Act 1961, ss 216B(2) and (3).

876 Crimes Act 1961, ss 216B(4) and (5).

877 Crimes Act 1961, s 216B(2)(a). Private investigators cannot rely on the participant monitoring exception to record their conversations with others without consent: Private Investigators and Security Guards Act 1974, s 52.

878 Crimes Act 1961, s 216A(2)(b) meaning of "party."

879 Harassment Act 1997, ss 4(1)(a) and (b).

880 Summary Proceedings Act 1957, ss 200A-200P. A tracking device is defined in s 200A as a device that, when installed in or on anything, can be used to ascertain the location of a thing or person, or whether something has been opened, tampered with or in some way dealt with. The tracking device regime is to be replaced by a surveillance device warrant regime upon the enactment of the Search and Surveillance Powers Bill 2008 (Part 3, subpart 1).

881 This can be contrasted with legal controls for the use of interception devices where there is both an offence and a warrant regime.

Monitoring data

9.20 The issue in relation to covert data surveillance is whether activities such as computer hacking and other unauthorised access, the use of spyware and RFID skimming are adequately covered by the four computer misuse offences in the Crimes Act 1961:

- accessing a computer system dishonestly or by deception and, without claim of right, obtaining advantage or benefit or causing loss to any other person,[882] or doing so with intent to obtain an advantage or benefit or cause a loss to any person;[883]
- damaging or interfering with a computer system;[884]
- making, selling, distributing or possessing software for committing crime;[885] and
- accessing a computer system without authorisation.[886]

Section 249: Accessing a computer system for a dishonest purpose

9.21 The definition of "access" is fairly broad and means "instruct, communicate with, store data in, receive data from, or otherwise make use of the resources of the computer system."[887] "Dishonestly" is defined in section 217 of the Crimes Act, in relation to any act or omission, as meaning "done or omitted without a belief that there was express or implied consent to, or authority for, the act or omission from a person entitled to give such consent or authority."

9.22 The other key element of the offence is whether the unauthorised access results in a person obtaining an advantage or benefit or whether it causes a recognised loss to the person affected. One issue is whether this requires some sort of financial or other tangible benefit. This question was raised in a High Court case where a man repeatedly accessed the email account of his former partner while he was an employee of the internet service provider for the account.[888] The High Court found that the term "benefit" is not confined to a benefit of a financial or pecuniary nature and that it is not a prerequisite to the offence that the access causes a disadvantage to another person:[889]

> A non-monetary advantage may nevertheless comprise a benefit. Such an advantage might, for example, be the acquiring of knowledge or information to which one was not otherwise entitled. The advantage might be the invasion of another's privacy. It might be knowledge or information that could be used to exploit another person. For example, wrongful accessing of the e-mail communications of another for the advantage of

882 Crimes Act 1961, s 249(1)(a).

883 Crimes Act 1961, s 249(1)(b).

884 Crimes Act 1961, s 250.

885 Crimes Act 1961, s 251.

886 Crimes Act 1961, s 252.

887 Crimes Act 1961, s 248.

888 *Police v Le Roy* (12 October 2006) HC WN CRI-485-58, Gendall J; *Le Roy v Police* (19 August 2008) HC WN CRI 485-38 Dobson J.

889 *Police v Le Roy* (12 October 2006) HC WN CRI 485-58, paras 11, 21 Gendall J.

disclosure. Or use for political purposes or purposes of embarrassment. Information obtained might also be used for the benefit or advantage of the wrongdoer in acting in a way so as to harass another in breach of the Harassment Act 1997, or be used to assist in the breach of a protection order under the Domestic Violence Act 1995.

9.23 The High Court held that, in the context of the relationship between the man and his former partner (taking account of a protection order enforcing the absence of contact) the man exploited a means of getting access that was not properly available to him and that accessing the email account gave him a meaningful benefit, irrespective of the extent to which he opened particular emails, or even considered the sender and the subject line indicating the nature of the content of individual emails.[890]

9.24 It is worth noting the argument of counsel before the court that the finding may mean that there is little to distinguish the requirements of section 249 from the simpler charge of unauthorised access to a computer system under section 252.

9.25 The case indicates that whether there is a benefit to the person dishonestly accessing the computer system may depend on the nature of the relationship between the people involved. The offence may not catch snooping into someone else's affairs by accessing the person's computer where there is no substantive relationship (or former relationship) between the person accessing the computer without authorisation and the target. However, one of the other offences may apply.

Section 250: Damaging or interfering with a computer system

9.26 The main issue under section 250 is whether there is damage or interference with a computer system. Trojan Horse spyware was considered in a case considering a charge of wilful damage (predating the computer misuse offences).[891] In that case, Judge Harvey held that the spyware did cause damage to the computer system, describing "damage" as an action by one person in respect of the property of another which (a) detrimentally affects the utility, appearance or function of the property, or (b) causes the property to perform or behave in a way unanticipated by the lawful owner or user, which (in both cases) requires intervention to restore the property to its original utility, appearance or functional state.[892] This suggests that malware such as Trojan Horse spyware will be considered to damage a computer system for purposes of section 250.

Section 251: Making, selling, distributing or possessing software

9.27 This offence applies to anyone supplying software that enables someone to access a computer system without authorisation, and which the supplier knows will be used for the purpose of committing a crime (such as one of the other computer misuse offences) or which the supplier promotes as being useful in the

890 *Le Roy v Police* (19 August 2008) HC WN CRI 485-38 paras 21-22, Dobson J.

891 *R v Garrett* [2001] DCR 955.

892 *R v Garrett* [2001] DCR 955, para 100. See also Judge David Harvey *Internet.law.nz: Selected Issues* (2 ed, LexisNexis, Wellington, 2005) 196-199 for discussion of damage in relation to a computer system.

commission of a crime.[893] There is also an offence for possession of software to access a computer system without authorisation where the person in possession of the software intends to use it to commit a crime.

Section 252: Accessing a computer system without authorisation

9.28 Section 252 will catch most computer hacking from outside a data-holding agency. But insider hacking will likely be exempt due to the exception to the offence providing that any person authorised to access a computer system for one purpose does not commit an offence if he or she accesses the computer system for an unauthorised purpose.[894] Unauthorised access may also be caught by section 249 if it is "dishonest' and amounts to a "benefit" to the person accessing the computer system (which may depend on the relationship between the people involved).

9.29 Unauthorised insider access is considered to be outside the scope of the Privacy Act, as the privacy principles impose obligations on the agency collecting or holding personal information, rather than on individual employees. Complaints under the Privacy Act about unauthorised insider access must be made about the conduct of the agency, rather than the actions of employees. This will include the actions of employees in the course of performing their duties;[895] however, where the unauthorised access is outside the scope of an employee's duties, complaints may be limited to whether the agency complied with its obligations in relation to storage and security of the information under principle 5.[896]

9.30 There are exceptions to section 252 for access under an interception or search warrant or under any other legal authority.[897] There are further exceptions for access by the New Zealand Security Intelligence Service under an interception warrant,[898] and access by the Government Communications Security Bureau under authority.[899] These exceptions do not apply to the other computer misuse offences.

SURVEILLANCE AND THE CIVIL LAW

9.31 Sometimes a complainant may be able to sue a person who has placed him or her under surveillance for damages, or to seek an injunction. Some of the possible causes of action follow.

893 For a U.S. example, see Chuck Miller "Keylogger Spyware Ordered off the Market" (17 November 2008) www.scmagazineus.com (accessed 23 November 2008) where the Federal Trade Commission brought an action against a Florida company to halt the sale of RemoteSpy keylogger spyware.

894 Crimes Act 1961, s 252(2). For discussion of the issue of insiders under the Computer Misuse Act 1990 (UK), see Neil MacEwan "The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future" [2008] Crim LR 955, 957-959.

895 Privacy Act, s 4.

896 The Privacy Commissioner has recommended a modification to principle 5 to better deal with unauthorised access from within a data-holding agency; see Privacy Commissioner *Necessary and Desirable – Privacy Act 1993 Review* (Office of the Privacy Commissioner, Wellington, 1998) recommendation 23.

897 Crimes Act 1961, s 252(3).

898 Crimes Act 1961, s 253.

899 Crimes Act 1961, s 254.

Trespass

9.32 Trespass to land and trespass to goods can sometimes provide remedies. For example, trespass can apply to unauthorised entry to install a camera (but will not apply where the camera is installed by someone authorised to be on the premises unless entry is obtained through some form of deception). However, in other cases, whether trespass applies will depend on the factual circumstances of the surveillance. As noted in *Hosking v Runting*:[900]

> Trespass may be of limited value as an action to protect against information obtained surreptitiously. Long-lens photography, audio surveillance and video surveillance now mean that intrusion is possible without a trespass being committed.

9.33 Although trespass is aimed at protecting property rights rather than privacy, damages awards in cases involving trespass to land have included compensation for invasion of privacy.[901] There is no such precedent in cases involving trespass to goods, where remedies are determined on the basis of reinstating or repairing the object.[902] Damages may therefore be minimal where the interference with goods involves a surveillance device which can easily be removed without damaging the goods involved. However, damages may also be awarded for upset and distress,[903] which could potentially provide redress for breach of privacy.

Nuisance

9.34 In disputes between neighbours involving visual surveillance of property, injunctions have been granted under the tort of nuisance. In an Ontario case, damages were awarded in nuisance for the deliberate invasion of privacy by the use of a surveillance camera in a neighbourhood dispute.[904] In a case in New South Wales, an interim injunction was granted and indefinitely extended to restrain the use of video surveillance equipment (including sensor flood lighting) that overlooked a neighbour's backyard, on the basis that the use of the video equipment was sufficiently close to "watching and besetting" to constitute an actionable nuisance.[905]

9.35 It is not clear whether a claim under the tort of nuisance would succeed in similar circumstances in New Zealand. According to *The Law of Torts in New Zealand*, while nuisance can be employed against an unreasonable interference with a person's right to the use or enjoyment of their land, the nuisance action does not "protect such privacy values as the right not to be spied upon; one cannot prevent a neighbour from looking over the fence to see

900 *Hosking v Runting* [2005] 1 NZLR 1 para 118 (CA) Gault P and Blanchard J.

901 See para 2.99 above.

902 Cynthia Hawes "Interference With Goods" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 467.

903 Cynthia Hawes "Interference With Goods" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 467.

904 *Lipiec v Borsa and Novak* (1996) 17 O.T.C. 64. In another Ontario case, a man was found guilty of criminal mischief for mounting a surveillance camera on the second story deck of his house which recorded all activity in his neighbour's yard on a 24 hour basis for a month: *R v Almeida* [2001] OJ No 5179 (Ont. SCJ).

905 *Raciti v Hughes* (1995) 7 BPR 14,837, 14,841 (NSWSC) Young J.

what is happening on one's land."[906] Nevertheless, surveillance that is so intrusive that it affects a person's enjoyment of his or her own property, such as continuous overt surveillance or surveillance involving floodlighting, could potentially be challenged on the basis of a claim of nuisance, although this would be breaking new legal ground in New Zealand.

Civil harassment

9.36 The Harassment Act 1997 provides the civil remedy of a restraining order for harassment by specified acts done on at least two occasions within a 12-month period. No provision is made for awards of damages. The Harassment Act is primarily concerned with overt acts, and may be difficult to apply to surreptitious surveillance.[907] It may also be difficult to apply to continuous surveillance, which could be considered to be a single act and therefore not within the scope of the Act.

Breach of confidence

9.37 The common law action of breach of confidence is outlined in chapter 2. Breach of confidence protects against the unauthorised use of information that has been imparted in confidence; however, it may also cover the unauthorised use or disclosure of information which is surreptitiously obtained. The Law Commission of England and Wales concluded in 1981 that it was "very doubtful to what extent, if at all, information becomes impressed with an obligation of confidence by reason solely of the reprehensible means by which it has been acquired."[908] However, in *Francome v Mirror Group Newspapers Ltd*,[909] the English Court of Appeal held that the doctrine of breach of confidence extended to an unlawful telephone tap used by a private person, suggesting that the doctrine will apply where the information is illegally obtained.[910] What is less clear is whether information obtained through means that are not unlawful may also fall within the scope of the doctrine.[911]

906 John Smillie "Nuisance" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 399.

907 For a case in which the Protection from Harassment Act 1997 (UK) was applied to covert surveillance see *Howlett v Holding* [2006] EWHC 41 (QB) Eady J; Olga Craig "Scrap Dealer Behind Five-Year Hate Campaign Faces £1 m Bill" (30 January 2006) *Telegraph* www.telegraph.co.uk (accessed 23 January 2009). In this case, the plaintiff became aware that the defendant was putting her under surveillance, but did not know whether she was under surveillance at any given time.

908 Law Commission *Breach of Confidence* (R 110, Cmnd 8388, London, 1981) para 4.10. Recommendation 6.46 set out the circumstances in which the Law Commission concluded that a person should owe an obligation of confidence in respect of information that has been improperly obtained (including from the use of surveillance devices). An exception was proposed for information obtained in the lawful exercise of an official function in regard to the security of the State or the investigation or prosecution of a crime. However, the proposals were not implemented.

909 *Francome v Mirror Group Newspapers Ltd* [1984] 1 WLR 892 (an interlocutory decision).

910 Megan Richardson "Breach of Confidence, Surreptitiously or Accidentally Obtained Information and Privacy: Theory versus Law" (1994) Melb LR 673, 674, 694. For a discussion of the meaning of illegality in relation to breach of confidence, see also George Wei "Surreptitious Takings of Confidential Information" (1992) 12 LS 302, 316-319.

911 See CD Freedman "Protecting Confidential Commercial Information through Criminal Law: Comments on Issues" (1999) 4 Comms L 87, 89.

9.38 In *Electronic Commerce Part One,* the New Zealand Law Commission concluded that a person who obtains confidential information by reprehensible means, such as hacking or interception, is subject to a duty of confidence, while noting that there is a degree of uncertainty.[912]

9.39 Breach of confidence therefore provides a possible civil remedy in respect of the use or disclosure of information obtained from covert surveillance, at least where the surveillance is prohibited by the criminal law. However, the doctrine is directed not to the intrusion caused by surreptitious information gathering but to the subsequent use of any such information:[913]

> [I]t seems odd to limit protection of that which is considered properly protectable, to acts of use or disclosure but not acquisition. Surely it is the nature of the misappropriative act itself that is culpable …

The doctrine will not be available in cases where the surveillance does not result in the gathering of confidential information, or where information is gathered but is not further disclosed or published. Even where illegally gathered information is disclosed, it is worth noting that there is a public interest defence to an action for breach of confidence.[914]

Privacy tort

9.40 The Court of Appeal decision in *Hosking v Runting* was limited to confirming the availability of a privacy tort for publication of private facts, and did not extend to establishing a remedy for intrusions into solitude or seclusion, although Gault P and Blanchard J acknowledged that existing laws will not always cover surreptitious surveillance.[915]

9.41 The publication tort may provide a remedy where the published information was obtained through covert use of a surveillance device and the publication is "highly offensive to a reasonable person." However, as the publication tort covers only part of the field, targets of surveillance may be left without an effective remedy for significant intrusions into their privacy where information obtained through surveillance is not published (or at least where there is no evidence that it is going to be published), where the particular criteria of the publication tort are not met, or where the material is obtained by one party through surveillance and is published by another.

912 New Zealand Law Commission *Electronic Commerce Part One: A Guide for the Legal and Business Community* (NZLC R50, Wellington, 1998) paras 161-166. See also New Zealand Law Commission *Electronic Commerce Part Two: A Basic Legal Framework* (NZLC R58, Wellington, 1999) paras 211- 216.

913 CD Freedman "Protecting Confidential Commercial Information through Criminal Law: Comments on Issues" (1999) 4 Comms L 87, 91.

914 However, disclosure in certain circumstances may nevertheless be an offence: see for example Crimes Act 1961, s 216C in relation to the disclosure of unlawfully intercepted communications.

915 *Hosking v Runting* [2005] 1 NZLR 1 para 118 (CA) Gault P and Blanchard J.

Breach of statutory duty

9.42 The civil cause of action for breach of statutory duty is outlined in chapter 2. This tort operates to provide a cause of action where a duty set out in statute is breached.[916] The tort could be a potential avenue for civil redress in relation to breaches of criminal offences prohibiting certain forms of surveillance.

9.43 Although occasionally the tort can be inferred where a statute does not explicitly provide a remedy in tort, the more satisfactory avenue is for the matter to be put beyond doubt by confirming in the statute that civil liability can flow from breach of the statutory offence. An example can be found in the Telecommunications Act 2001, which specifies liability for damages for connecting unauthorised equipment to a telecommunications network.[917]

9.44 Such a provision was included in the Listening Devices Bill which was introduced in 1975 but never passed. Clause 25 of the Bill provided for the award of damages to a person whose private communication had been unlawfully intercepted or disclosed. It specified that, in assessing damages, the court could take into account any distress, annoyance or embarrassment suffered or likely to be suffered by the plaintiff as a result of the unlawful conduct.[918]

9.45 At the time the computer misuse offences were formulated, the Law Commission asked whether a statutory tort should be introduced that would give the owner of a computer system a right of action against a person where that person had breached criminal legislation dealing with computer misuse and, as a result, caused loss or obtained a benefit.[919] However, at that time the Law Commission received very few submissions and decided not to make a recommendation on this point.[920]

Civil remedies under the Telecommunications Act

9.46 The Telecommunications Act 2001 contains civil remedies in relation to the unauthorised connection of equipment (such as equipment used to intercept telecommunications and telephone analysers used to obtain call data) to a telecommunications network. Any person who breaches the prohibition is liable for damages (subject to a three-year limitation period).[921]

9.47 The section does not specify who may sue for damages. The predecessor to the section provided that any person suffering loss or damage as a result of the conduct could sue for damages as if the conduct constituted a tort.[922] Section 111 of the

916 See John Burrows "Breach of Statutory Duty" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington 2005); KM Stanton *Breach of Statutory Duty in Tort* (Sweet & Maxwell, London, 1986).

917 Telecommunications Act 2001, s 110.

918 Hon Dr A M Finlay (25 July 1975) 400 NZPD 3413.

919 New Zealand Law Commission *Electronic Commerce Part Two: A Basic Legal Framework* (NZLC R58, Wellington, 1999) paras 231-234; New Zealand Law Commission *Electronic Commerce Part Three: Remaining Issues* (NZLC R68 Wellington, 2000) para 73.

920 New Zealand Law Commission *Electronic Commerce Part Three: Remaining Issues* (NZLC R 68, Wellington, 2000) para 75.

921 Telecommunications Act 2001, s 110.

922 Telecommunications (Residual Provisions) Act 1987, s 20D, as repealed by Telecommunications Act 2001, s 159(1).

Telecommunications Act provides for injunction applications to restrain conduct that would breach the prohibition, though only the network operator can apply for an injunction. It could be inferred that the limitation of the injunction remedy to network operators implies that the damages remedy is intended to apply more widely to anyone affected by the breach of the prohibition.

REGULATORY CONTROLS

Privacy Act

9.48 The Privacy Act is concerned primarily with information privacy. Surveillance can often, but may not always, infringe informational privacy. As noted by the Irish Law Reform Commission:[923]

> There is no necessary connection between surveillance and the collection of information. As surveillance is considered intrusive in itself, regardless of any information-collecting purpose, mere regulation of the use of information obtained by surveillance is likely to be considered insufficient protection of privacy.

9.49 The extent to which the Privacy Act 1993 applies to surveillance is discussed in chapter 3.[924] As we noted, some commentators have raised questions about the application of the collection principles (principles 1-4) to information-gathering using surveillance devices. One question is whether surveillance involves the collection of personal information in terms of the Act's definition of "collect"; another is whether, for the purposes of principle 2, information obtained by surveillance is collected "directly from" the individual concerned.

9.50 The Parliamentary debates preceding enactment of the Privacy Act suggest that the Act was not intended to cover the whole field of privacy, and it was recognised that issues of surveillance needed to be considered further at a later time:[925]

> [S]nooping or prying into people's private affairs, whether by electronic eavesdropping or by entry on to private property by telephoto lenses or other technological devices, probably at some time would need further consideration by the House.

9.51 Nevertheless, the Privacy Act is applied to the gathering of information by surveillance by the Privacy Commissioner and the Human Rights Review Tribunal. Of particular relevance is principle 4:

> Personal information shall not be collected by an agency –
>
> (a) by unlawful means; or
>
> (b) by means that, in the circumstances of the case,–
>
> (i) are unfair; or
>
> (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

923 Irish Law Reform Commission *Privacy: Surveillance and the Interception of Communications* (Dublin, 1998) 9.

924 Paras 3.6-3.14.

925 Hamish Hancock (18 March 1993) 533 NZPD 14132. See also Peter Dunne (20 April 1993) 534 NZPD 14731: "the increasing prominence of electronic eavesdropping … is not addressed in the Bill, but … it would be wrong to assume that it has been ignored. It is an issue that will become increasingly prevalent in the future … It is something that, at some point in the ongoing development of a comprehensive privacy law, we will have to make some decisions on, and we will have to enact legislation to give protection to individuals in relation to the implications thereof."

9.52 For example, the Privacy Act's information privacy principles may apply to the use of hidden cameras (but not to the act of installing the camera). The Privacy Commissioner has considered instances of hidden camera use in the workplace, for example, finding that the surveillance was permissible in the circumstances.[926]

9.53 It is worth noting that the principles impose obligations on "agencies."[927] While an individual can be an agency, where an agency is a body of persons such as a company, business or government department, it is the agency that must comply with the principles, rather than individual employees.[928]

9.54 Section 56 of the Privacy Act (the domestic affairs exception) is also significant in the context of surveillance by individuals:

> Nothing in the information privacy principles applies in respect of –
>
> (a) the collection of personal information by an agency that is an individual; or
>
> (b) personal information that is held by an agency that is an individual,–
>
> where that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs.

9.55 The exception has been interpreted fairly broadly to exempt collections of personal information by individuals for their own personal affairs and potentially excuses much surveillance by private individuals, such as the use of cellphone cameras. The Law Commission has previously recommended that section 56 should be amended so that it does not cover information obtained through criminal offending such as intimate visual recording.[929] The section 56 exception also excuses any disclosure, provided the collection and holding of personal information is for personal, family or household affairs (although disclosure may be indicative that the information collection was outside the scope of the exception).

9.56 To date, the Privacy Commissioner has encouraged self-regulation in relation to privacy issues arising through the use of technologies such as CCTV and RFID.[930] The Privacy Commissioner has not, therefore, issued any specific guidelines or a Code of Practice for surveillance generally or CCTV surveillance in particular.[931] However, work is currently being done by the Office of the Privacy Commissioner on specific guidance for CCTV surveillance.

---

926 *Employee Objects To Employer Installing Video Camera In Locker Room* [2003] NZ PrivCmr 25 – Case Note 32277. The use of hidden cameras by employers is also governed by employment law concepts such as the obligations of trust, confidence and good faith, and procedural fairness where surveillance footage is used to discipline or dismiss an employee: see chapter 12 below.

927 Privacy Act 1993, s 2(1) (definition of "agency").

928 Privacy Act 1993, s 6. Under s 4, the actions of an employee in the performance of their duties are to be treated as the actions of the agency.

929 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) para 4.54.

930 See, for example, the Police CCTV policy discussed at para 9.64 and the voluntary RFID Code of Practice discussed at para 9.67.

931 The Privacy Commissioner has issued a pointer on video surveillance in the workplace which is reproduced in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, 2008) PVA.6.7(e), EPM.3.5.

BSA standards

9.57 The Broadcasting Standards Authority intrusion principle (privacy principle 3) is concerned with how information is collected, although the principle is triggered by the disclosure of information by broadcasting material obtained in an intrusive manner.[932] The publication by broadcasters of material obtained through the use of surveillance devices in a way that interferes with a person's solitude or seclusion may therefore breach the intrusion principle, if the intrusion would be highly offensive to a reasonable person and is not outweighed by the public interest in the disclosure.

9.58 For example, the broadcast of material obtained from hidden cameras is subject to the BSA privacy intrusion principle.[933] However the principle does not apply to the broadcast on the internet of material from hidden cameras. Nor does it apply to the use of hidden cameras where the material obtained is not broadcast.

9.59 The use of covert recording devices by the broadcast media may also breach the BSA's Fairness standards.

9.60 Overt filming is likely to be less intrusive than surreptitious filming.[934] The public place exemption will also allow most filming in public places, unless the subject is particularly vulnerable.[935]

Press Council

9.61 The Press Council Statement of Principles includes a principle that "Everyone is entitled to privacy of person, space and personal information", subject to a public interest exception. This, by virtue of reference to "space", is broadly-enough framed to cover intrusive behaviour such as surveillance, although again the Council's jurisdiction is unlikely to be invoked unless material obtained by such behaviour has been published. The principle concerning the use of "misrepresentation, deceit or subterfuge" would also seem to require that publications avoid the use of hidden recording devices, except where the story is clearly in the public interest and the information can be obtained in no other way. The only sanction available to the Council, which is not a statutory body, is to require an offending publication to publish the essence of a decision against it.

932 See para 3.46 above.

933 *Drury and Daisley v TV3 Network Services Ltd* (10 October 1996) Broadcasting Standards Authority 1996-130, 1996-131, 1996-132; *O'Connell v TVWorks Ltd* (25 June 2008) Broadcasting Standards Authority 2007-067; *TVNZ v KW* (27 June 2007) Broadcasting Standards Authority 2006-087; *CanWest TVWorks Ltd v XY* [2008] 1 NZAR 1 (HC).

934 Stephen Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 118-119.

935 Stephen Price *Media Minefield: A Journalist's Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 120-121.

Marketing and market research industry standards

9.62 Both the Marketing Association and the Market Research Society have codes of practice that deal, among other things, with the recording of information. The Marketing Association's code provides that consumers must be informed when phone conversations are being recorded.[936] Marketing organisations are also required to have a complaints handling procedure.[937]

9.63 The Market Research Society's Code provides that respondents must be informed before observation techniques or recording equipment are used for research purposes, except where these are openly used in a public place and no personal data is collected.[938] There is a complaints process whereby complaints about breaches of the Code can be referred to the Society.

Police CCTV policy

9.64 The New Zealand Police have, in consultation with the Privacy Commissioner, issued a policy to provide guidance in the setting up of CCTV systems for crime-prevention purposes.[939] This includes an example of a CCTV public notice and a compliance checklist. Key features of the policy include community consultation prior to the installation of cameras, clear signage of camera locations, no tracking or zooming in on members of the public, limited purposes for the surveillance, erasure of recorded material within two months unless needed as evidence, and access to footage by individuals who have been recorded, if the footage is readily retrievable.

Local government CCTV policies

9.65 Several local councils have developed CCTV strategies and policies. For example, the Hastings District Council, the Hastings Crime Prevention Camera Trust and Hastings Police have developed a Hastings District Operating Policy to serve as a best practice guide for the operation and expansion of the Hastings District CCTV system. This sets out which entity is responsible for each aspect of the system, including signage, records, security and retention of footage, control and operation of cameras, use of recorded information, access to recorded information by anyone filmed, and a complaints procedure. A similar policy has been developed for the Whakatane District.[940]

9.66 Manukau City Council is developing a CCTV policy which is to contain processes to comply with advice from the Privacy Commissioner and with the Police CCTV protocols.[941] Due to frequent requests for footage from private CCTV

936 New Zealand Marketing Association *Code of Practice for Direct Marketing in New Zealand* (revised November 2006) www.marketing.org.nz (accessed 17 December 2008) principle 5(b).7.

937 New Zealand Marketing Association *Code of Practice for Direct Marketing in New Zealand* (revised November 2006) www.marketing.org.nz (accessed 17 December 2008) principle 5(a).1.

938 Market Research Society of New Zealand Inc *Code of Practice* (revised June 2008) www.mrsnz.org.nz (accessed 17 December 2008) article 6.

939 New Zealand Police *Policy on Crime Prevention Cameras in Public Places* (updated November 2003) www.police.govt.nz (accessed 14 April 2008).

940 Whakatane District Council *Whakatane District Electronic Surveillance (Closed Circuit Television) Policy,* adopted 13 December 2006.

941 Manukau City Council *Closed Circuit Television Camera (CCTV) Strategy* April 2006, recommendation 8.

systems, and to facilitate sharing of such footage, the Council's CCTV strategy also recommended that a feasibility study be undertaken into establishing a bylaw that would require registration of all privately-owned CCTV systems within Manukau.[942]

Voluntary RFID Code of Practice

9.67 GS1 in New Zealand has created a voluntary RFID Consumer Protection Code of Practice,[943] based on the EPCglobal Guidelines on EPC (electronic product code) for Consumer Products. This requires participating retailers to give notice and information to consumers, as well as the option of tag removal or deactivation. One provision restricts retailers from scanning RFID tags from other businesses without the consumer's consent. The Code also contains a complaints resolution process. The Privacy Commissioner has said that she will be watching to see whether a compulsory code is needed to protect customers.[944]

BILL OF RIGHTS ACT

9.68 The question of whether the use of mass surveillance (such as CCTV) in public places by public agencies could engage section 21 of the New Zealand Bill of Rights Act 1990 (the right not to be subjected to unreasonable search and seizure) has not been tested. Similarly in Canada "there is still no clear answer from the courts as to whether this type of surveillance [CCTV] constitutes a 'search' within the meaning of s. 8 of the Charter [of Rights and Freedoms]."[945] In the United States, "federal courts have yet to seriously address the question of how to analyze [public video surveillance] under the Fourth Amendment."[946] Although it may be difficult to establish any reasonable expectation of privacy in a public place for this purpose, some argue that CCTV can affect the relationship between citizen and the State due to the asymmetry of observation,[947] the continuous nature of the surveillance, the effect on anonymity and the invasiveness of multiple surveillance techniques used together.[948] It is conceivable that a public CCTV system could give rise to considerations of reasonableness under section 21, depending on the nature and capabilities of the system (that is, how many additional technological enhancements it uses), how the system is operated

942 Manukau City Council *Closed Circuit Television Camera (CCTV) Strategy* April 2006, recommendation 35, section 6.

943 GS1 New Zealand Inc *EPC/RFID Consumer Protection Code of Practice* www.gs1nz.org (accessed 1 December 2008).

944 Rachel Bowie "Day of the RFIDs" (September 2007) *Consumer New Zealand* 40, 41.

945 Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta Law Review 43, 66.

946 Marc Jonathan Blitz "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity" (2004) 82 Tex L Rev 1349, 1359.

947 See Marc Jonathan Blitz "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity" (2004) 82 Tex L Rev 1349, fn 35: "As a number of commentators have noted, searches by far-away camera operators may be even more intrusive in one respect than on-site physical searches because an unobserved camera operator is less likely than a police officer acting in full view of others to have qualms about scrutinizing people in ways that conflict with widespread social norms."

948 Robert W. Hubbard, Susan Magotiaux and Matthew Sullivan 'The State Use of Closed Circuit TV: Is there a Reasonable Expectation of Privacy in Public?" (2004) 49 CLQ 222, 244-245.

and how the collected footage is used.[949] Section 21 may therefore provide some general control on policies and practices in relation to public CCTV systems, but this is by no means clear.[950]

9.69 Like all the rights and freedoms in the Bill of Rights, those protected under section 21 may be subject "to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[951] Surveillance which meets that reasonableness criterion does not breach the Bill of Rights Act.

SURVEILLANCE SCENARIOS

9.70 We now set out a series of scenarios with a brief discussion of the law that may currently apply in each case.

Scenario 1: visual surveillance into private property (interior)

9.71 ***A**, a private individual who is seeking evidence for a lawsuit, rents a room in a house adjoining **B**'s residence. For two weeks **A** looks into the windows of **B**'s living room through a telescope and takes pictures with a telescopic lens.*[952]

9.72 If **A** is a private investigator, the taking of the photographs would be an offence under section 52 of the Private Investigators and Security Guards Act 1974. If **A** is not a private investigator, it is uncertain whether any legal remedy would be available to **B**. If the pictures were not of an intimate activity, there would be no intimate visual recording offence. The peeping and peering offence could apply to the use of the telescope, but only at night.

9.73 Under principle 4 of the Privacy Act, the use of the telescope and the photography could be considered to intrude to an unreasonable extent on **B**'s personal affairs, so **B** could make a complaint to the Privacy Commissioner that there has been an interference with his privacy. However, the Privacy Act may not apply (depending on the nature of the lawsuit) as the section 56 exemption permits the collection of personal information in connection with an individual's personal affairs.

9.74 If **A** had been a law enforcement officer instead of a private individual, the legal position would currently be no different. However, if the Search and Surveillance Powers Bill is passed in its current form, law enforcement officers will require warrants to carry out visual surveillance of private activity in private buildings.[953]

949 Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta L Rev 43, 67.

950 The Council of Europe has initiated a study on public surveillance and proposes to issue guidelines for balancing the public interests involved against the human rights and freedoms of the individual: European Commission for Democracy through Law (Venice Commission) *Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights* (Study No. 404/2006, Strasbourg, 23 March 2007) para 5.

951 New Zealand Bill of Rights Act 1990, s 5.

952 This scenario is adapted from one cited by the American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652B.

953 Search and Surveillance Powers Bill 2008, no 300-1, cl 46(b).

Scenario 2: visual surveillance into private property (garden)

9.75 ***C** is a well-known actress. She is sun bathing topless beside the swimming pool in her own garden surrounded by a high fence. **D** is a fan. He climbs up a tree quite distant from her garden and with a telephoto lens takes a photograph of **C**.*[954]

9.76 The high fence would support **C**'s reasonable expectation of privacy for the purposes of the intimate visual recording offence.[955] That offence would apply to pictures taken where **C** was topless or naked or wearing underclothes, but not where she is wearing a swimsuit, or is clothed. If **D** observed **C** without taking pictures, the peeping and peering offence may not apply where **C** is in her garden rather than inside her home (and would not apply in any event to daytime observation).

9.77 **C** could make a complaint to the Privacy Commissioner that her privacy has been interfered with in breach of principle 4. However, as a private individual, **D** could seek to rely on the exemption in section 56 for the collection of information principally for his own personal affairs.

9.78 Watching **C** at her home is an act specified in the Harassment Act. If **D** repeats the same activity or commits another specified act (such as following **C**) within a period of 12 months, **C** could apply for a restraining order against him.

Scenario 3: visual surveillance affecting neighbours

9.79 *Friction between neighbours over alleged damage to a shared retaining wall results in neighbour **E** installing a rooftop surveillance camera to watch both backyards, 24 hours per day. The camera records neighbour **F**'s children swimming in the pool with their friends. Neighbour **F** feels that her family, and especially her children, are being subjected to unwanted surveillance.*[956]

9.80 If the Search and Surveillance Powers Bill is passed as currently drafted, law enforcement agencies would require a warrant to undertake visual surveillance of the curtilage of a private dwelling only if the period of surveillance exceeds three hours in 24, or eight hours in total. Periods less than this would not require a warrant.[957] But what is the case if, as here, private individuals undertake surveillance of the area around a private dwelling? The law is somewhat unclear, but the persons subject to surveillance may often have no remedy.

9.81 The camera surveillance may be an actionable nuisance, although there is no New Zealand authority. The surveillance could be civil harassment under the Harassment Act 1997 (watching a person's place of residence), for which an application for a restraining order could be made. However, civil harassment only applies if there are acts of harassment on two separate occasions. Continuous surveillance may be construed as one act.

954 This scenario is a modified version of a scenario used in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19 Wellington 2008) 211 (Example 3).

955 Crimes Act 1961, 216G(1)(a)(i).

956 Based on the report by Karen O'Shea "New Heights for Invasion of Privacy?" (30 August 2008) http://blog.silive.com (accessed 1 September 2008).

957 Search and Surveillance Powers Bill 2008, no 300-1, cl 46(c).

9.82 A complaint could be made to the Privacy Commissioner under principle 4 (that the collection of personal information intrudes to an unreasonable extent upon the personal affairs of the individual concerned). However, the domestic affairs exception in section 56 of the Privacy Act may allow neighbour **E** to argue that the primary purpose of the surveillance is to protect his own property and security, and that the privacy principles do not apply.

Scenario 4: photography in a public place

9.83 ***G** is sunbathing topless on a public beach topless when **H** photographs her with the camera on his cell phone.*[958]

9.84 Generally, there is no restriction on photographing or otherwise recording images in a public place. A common assumption is that there is no reasonable expectation of privacy with regard to photography and filming in such places. The question here is whether the circumstances and the purpose of the photography make any difference.

9.85 The summary offence of offensive behaviour in a public place may apply to the photography, depending on the circumstances. Intimate photography in a public place (other than up-skirt filming) is not covered by the intimate visual recording offence. The Harassment Act would not apply where only one photograph is taken. If **H** takes photographs of **G** on other occasions within a 12-month period, she could apply for a restraining order. However, it is not clear that taking a photograph in a public place would be considered a specified act under the Harassment Act.

9.86 A complaint to the Privacy Commissioner that the photography breaches principle 4 would not be likely to succeed. The photography is unlikely to be "unfair" (where it is not covert) and is unlikely to intrude upon **G**'s personal affairs where she is photographed at a public beach. In any event, **H** may well be able to rely on section 56 of the Privacy Act where he takes the photographs for his own personal affairs (that is, not for sale), in which case the Privacy Act principles will not apply.

Scenario 5: covert photography by media

9.87 *After months of speculation, including multiple references to an affair in mainstream political blogs, a newspaper carries a report suggesting that **I**, a senior public official, is having marital difficulties and is to separate from his wife. **I** has spoken publicly on the importance of family and the social problems associated with absent fathers. Following the story, **I** is ambushed by the media when leaving his office, but declines to comment and asks journalists to respect his and his children's privacy. Subsequently a newspaper photographer waits on a public reserve bordering **I**'s property and, using a long-lens camera, secretly takes a photograph of **I** and his wife in a tense conversation in their back garden. Another photographer working for the same newspaper waits outside the school attended by **I**'s children, and secretly photographs*

958 See New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 210, noting the unlikelihood of a remedy in this scenario under the current law. For discussion of the issues in this scenario, see Kelley Burton "Erosion at the Beach: Privacy Rights Not Just Sand" [2006] PLPR 3.

*them with a long-lens camera as they leave the school grounds. The images are published alongside an article rehashing the earlier story and rehearsing **I**'s previous statements on the importance of family.*

9.88 The news media exemption from the Privacy Act means that **I** could not complain to the Privacy Commissioner. Neither of the photographers has committed an offence, nor have they trespassed as they have remained on public property. **I** could bring a complaint to the Press Council. He could also bring a tort claim for invasion of privacy by publication of private facts. This claim might succeed in relation to the publication of photographs of **I** and his wife on private property where they have a reasonable expectation of privacy, although the newspaper could seek to rely on the defence of legitimate public concern in the publication of the photographs. It is unlikely, based on the Court of Appeal decision in *Hosking*, that the photographing of **I**'s children in a public place would be found to be an invasion of privacy.

9.89 The application of the Harassment Act to these facts is not straightforward. It is likely that watching and loitering near **I**'s house and his children's school would be considered to be two separate specified acts for the purposes of the Act. It is clear from the Act that a specified act done to one of **I**'s family members, due wholly or partly to that person's family relationship to **I**, should be treated as an act done to **I**.[959] Therefore, if the same person committed both acts, **I** could seek a restraining order against that person. In this case, two separate photographers are involved, but both are working for the same newspaper. **I** could, therefore, seek a restraining order against the media company that owns the newspaper, or perhaps against the individual who commissioned the photographs.[960] If a court were to make such an order, it could direct that it also apply to any freelance photographers who have been commissioned by the newspaper to pursue **I** and his family.[961] However, the media organisation could seek to rely on the defence that the specified acts were carried out for a lawful purpose.[962]

Scenario 6: overt visual surveillance by media

9.90 ***J** is a well-known and respected television personality who has spoken publicly about the dangers of using illicit drugs. However, following an acrimonious split, her ex-partner alleges that **J** is a cocaine addict. **J** issues a statement denying the allegation, but refuses to discuss the matter further with the media. Representatives of a range of print and broadcast media organisations pursue her whenever she appears in public, filming and photographing her and asking her questions. They also wait outside her house, filming and asking her questions whenever she emerges.*

959 Harassment Act 1997, s 5.

960 The Harassment Act 1997 does not limit the meaning of "person" to a natural person, and section 16(2) of the Act provides that a restraining order may be made in respect of a respondent who encourages another person to do a specified act to the applicant.

961 Harassment Act 1997, s 18(1), provides that if the Court makes a restraining order against the respondent, it may direct that the order also apply against any other person if the respondent is encouraging, or has encouraged, that person to do any specified act to the applicant. Section 19(1)(b) makes it a standard condition of restraining orders that the respondent must not encourage any person to do a specified act to the person for whose protection the order is made, if the specified act would be prohibited by the order if done by the respondent.

962 Harassment Act 1997, s 17.

9.91 No offence is committed in this scenario, and there is no trespass as the media only film **J** when they are on public property. The principles of the Privacy Act do not apply to the news media in their news activities. As in Scenario 5, the application of the Harassment Act is complex. The media's actions would, if carried out by or at the encouragement of a single person, fall within the meaning of "specified acts" in the Harassment Act. However, in this case the actions are carried out by an ever-changing "media pack", made up of representatives of various media organisations. The Harassment Act does not seem to be well-suited to dealing with such a situation. The media could also seek to use the Act's defence of lawful purpose. **J** could complain to the Press Council and the BSA about the media's activities.

Scenario 7: covert filming at a private party

9.92 ***K** is a high-profile New Zealand sportsman who attends a private party while on tour. Using a cellphone camera, **L** (a fellow partygoer) records footage which shows **K** apparently engaged in a sexual act with a man. The footage is offered to various media organisations for a fee, but before any mainstream media purchase or publish the images, the video appears on an overseas-hosted gay website. The New Zealand media publish this fact and reproduce stills from the video, taken from the website. International media follow suit. **K** is outraged by what he sees as an invasion of his privacy. He denies that the video shows him engaged in a sexual act, although most viewers of the video believe that it does.*

9.93 It is possible that this scenario could lead to a prosecution under the intimate covert filming provisions of the Crimes Act 1961, but there are two potential obstacles to such a prosecution. First, while **K**'s denial that the video shows him "engaged in an intimate sexual activity"[963] would not prevent a prosecution, it might make it difficult to obtain a conviction. Secondly, there could be a question about whether **K** was "in a place which, in the circumstances, would reasonably be expected to provide privacy"[964] when he was attending a crowded party, even if the video was taken at a semi-secluded location within the party venue. Potentially, however, **L** could be prosecuted for making, possessing, publishing, exporting and selling an intimate visual recording.[965] The New Zealand media organisations that publish images from the video could also be prosecuted for publishing an intimate visual recording. In addition, once New Zealand internet service providers are made aware that the video is an intimate visual recording (assuming it is found to be so), it is possible that they could be liable for publishing it if they fail to block access to websites carrying the images.[966]

9.94 **K** could complain to the Privacy Commissioner about **L**'s actions in recording and distributing the video. **L** could argue that the privacy principles do not apply as the video was made for his own personal use,[967] but this argument would carry little weight if it could be shown that he had tried to sell the footage. The news media exemption from the Privacy Act means that a complaint to the Privacy Commissioner

963 Crimes Act 1961, s 216G(1)(a)(ii).

964 Crimes Act 1961, s 216G(1)(a).

965 Crimes Act 1961, ss 216H-216J.

966 Crimes Act 1961, s 216K(3)(b) exempts internet service providers from the prohibition on publishing intimate visual recordings, but only if the provider does not know or suspect that a visual recording is an intimate visual recording.

967 Privacy Act 1993, s 56.

about the media's publication of the images would not succeed, but a complaint could be taken to the Press Council or the BSA. **K** could also sue both **L** and the media for invasion of privacy under the *Hosking* tort, or for defamation.

Scenario 8: release of CCTV footage

(a) suicide attempt

9.95 *A man suffering from depression attempts suicide with a kitchen knife in a public street. He is unaware that, following the attempt, he has been filmed by a local authority CCTV camera. Images extracted from the CCTV footage are published to support favourable publicity for Police use of CCTV surveillance and are broadcast on television, with inadequate masking of the man's face (he is recognisable to those who know him), and in a trailer for a crime programme the man's face is not masked at all.*[968]

(b) voyeuristic material

9.96 *CCTV cameras watching over a deserted civic area one night catch an amorous couple on film. The operator targets the camera on their sexual activity and takes a copy of the footage which he shares with friends and colleagues.*[969]

9.97 It is likely that the filming in these cases would not in itself be subject to any sanction, as the conduct took place in public. It is the use and disclosure of the images obtained which might be subject to legal redress, either under the Privacy Act (use or disclosure for a purpose other than that for which the information was collected), the Broadcasting Act (via a complaint to the BSA about the broadcast in scenario (a)), or the *Hosking* tort.

Scenario 9: activating web camera

9.98 ***M** purchases software which allows him to activate a web camera attached to a PC and view images from the camera remotely. He installs the software on **N**'s computer and uses the software to activate the camera so that he can watch **N** without her knowledge.*[970]

9.99 Although the web camera is not hidden, it is used to monitor **N** without her knowledge or consent. If the web camera is used to observe **N** in circumstances in which she has a reasonable expectation of privacy and is naked, semi-naked or engaged in one of the types of intimate activity specified in section 216G of the Crimes Act, **M** could have committed the offence of making an intimate visual recording. The fact that the images are transmitted in real time and not stored does not prevent him from being liable for this offence.[971] It would have

968 This scenario is based on the facts in *Peck v United Kingdom* [2003] ECHR 44.

969 See "A Hotbed of Groping" (13 August 2008) *Capital Times* Wellington 3, reporting on requests by TV news for groping footage from council security cameras in Civic Square in Wellington. According to Wellington City Council, footage is usually only released to police. See also Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta L Rev 43, 55-56, discussing an English film comprising of a montage of video clips from British CCTV systems including public displays of sexual intimacy.

970 This scenario is from the Australian Government, Department of Communications, Information Technology and the Arts *Spyware Discussion Paper* (May-June 2005) 15.

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

to be shown that he made the intimate visual recording intentionally or recklessly.[972] It is not an offence for **M** to watch **N** covertly via the camera if **N** is in a place where she does not have a reasonable expectation of privacy, or if the images are not intimate in nature. If the camera had an audio function that allowed **M** to overhear **N**'s private conversations, or if it allowed him to read her private written communications, he could be charged with an interception offence under the Crimes Act. The surreptitious installation of spyware may be a computer misuse offence, either accessing a computer system for a dishonest purpose, damaging or interfering with a computer system or unauthorised access to a computer system.

9.100 The Privacy Act principles are broad enough to apply to the collection of personal information even if it is not recorded. The surreptitious observation through a webcam may breach principle 4 on the grounds that it is unfair, or intrudes to an unreasonable extent on the personal affairs of the person being observed.

Scenario 10: covert audio recording

9.101 *Company X employs a private investigator to investigate an activist group that is believed to be planning to disrupt the company's activities. The private investigator uses a paid informant, **O**, to infiltrate the activist group. **O** joins the group and participates in its planning meetings and protest actions, as well as social functions with group members. She secretly makes audio recordings of conversations with group members, including conversations relating to their personal lives. These recordings are passed on to the private investigator, who also makes them available to Company X. Eventually the group members discover that **O** is an informant who has been recording their conversations, and complain that their privacy has been invaded.*

9.102 Under the Crimes Act 1961 it is an offence intentionally to intercept (which includes recording) a private communication using an interception device. However, it is not an offence for a person who is a party to a private communication to intercept that communication.[973] Thus, **O** would be committing an offence if she used her recording device to record a conversation in which she was not a participant (perhaps one taking place in another part of a room she was sitting in). It would not be an offence for her to record a conversation in which she was taking part, or to transmit such a conversation to a third party as it was taking place.

9.103 If the audio recording had been done by the private investigator himself, this would have been an offence under section 52 of the Private Investigators and Security Guards Act 1974. This Act regulates private investigators and their responsible employees. The activists could lay a complaint that **O** has been employed as a responsible employee of the private investigator without the necessary certificate of approval, which is an offence under the Act.[974] However,

972 Crimes Act 1961, s 216H.

973 Crimes Act 1961, s 216B.

974 Private Investigators and Security Guards Act 1974, s 34(3)(a) and (b).

in a decision on such a complaint, the Registrar of Private Investigators and Security Guards ruled on a number of grounds that two paid informants of a private investigation company were not employed by the company.[975]

9.104 The activists could complain to the Privacy Commissioner that information about their personal affairs had been collected unfairly, and perhaps unlawfully, in breach of information privacy principle 4. They could also complain that the covert nature of the recording is in breach of the requirements in information privacy principle 3 for notification that collection of personal information is taking place.

Scenario 11: participant recording

9.105 *A market researcher conducting a lengthy phone survey which asks consumers a number of personal questions such as their age, size of family, salary range, religious and political affiliations, omits to tell people surveyed that the calls are recorded to facilitate the compiling of responses.*

9.106 Although the telephone conversation between the consumer and the market researcher is a "private communication", no interception offence is committed as the recording of the survey by the marketing company is within the participant monitoring exception.[976]

9.107 The Privacy Act information privacy principles would apply to the collection of information for the survey. The omission to tell people that calls are being recorded would likely breach principle 3(1)(a) (an agency is to take reasonable steps to ensure that an individual is aware of the fact that information is being collected) and a complaint could be made to the Privacy Commissioner by those affected.[977] The omission would also breach the Market Research Society Code of Practice and a complaint could be made to that society.[978]

Scenario 12: cellphone monitoring

9.108 *A husband who suspects his wife is having an affair buys her a new internet-capable cellphone and installs spyware on the phone before he gives it to her. The spyware enables the husband to identify her incoming and outgoing calls, and to check text messages and mobile mail via an internet account.*[979]

---

975 *Morse v Thompson & Clark Investigations Ltd* (March 2008) Registrar of Private Investigators and Security Guards PI 700633, paras 15-16.

976 Crimes Act 1961, ss 216B(1)(a) and 216A(2).

977 While the consumers in this scenario are clearly aware that information is being collected, it is likely that principle 3 requires that they should also be told that they are being recorded. The Privacy Commissioner has commented, albeit in relation to quite different circumstances, that "making a tape recording would collect more information than merely listening to a conversation and would also open up additional purposes for which the information could be used. The fact of recording an interview on tape, rather than merely relying upon written notes and memory, is a matter that the individual should be made aware of under principle 3." *Employee Objects to Employer's Hidden Tape Recording in Theft Investigation* [2001] NZPrivCmr 6 – Case Note 16479.

978 Market Research Society of New Zealand Inc *Code of Practice* (revised June 2008) www.mrsnz.org.nz (accessed 17 December 2008), Article 6.

979 Leigh van der Stoep "Spying on your partner just got easier" (21 September 2008) *Sunday Star Times*; "Why Spying on Spouses May be a Really Bad Call" (28 September 2008) *Sunday Star Times*; Catch a Cheating Spouse www.flexispy.com (accessed 7 October 2008). See also Brian Krebs "When Hackers Attack: Practicing Cybersecurity at Home" (January 2009) *Popular Mechanics* www.popularmechanics.com (accessed 16 December 2008).

9.109 Assuming that the text messages are not intercepted in transit but on receipt by the cellphone, the interception offence will not apply. In any event, it is unclear whether the spyware would be an "interception device", although the wife's cellphone could be construed as the "interception device" when monitored by her husband.[980]

9.110 The downloading of the spyware might be a computer misuse offence. This depends partly on whether the cellphone is a "computer", a term that is not defined in the Crimes Act. The view of Judge Harvey is that a mobile phone could be classed as a computer.[981] The computer misuse offences would not apply, however, where the spyware is downloaded while the cellphone is under the husband's ownership and control. Nevertheless, those offences could apply in different circumstances where spyware is downloaded to a cellphone belonging to someone else.

9.111 Another issue is whether the use of spyware to obtain call data such as records of incoming and outgoing calls gives rise to any liability. The Telecommunications Act 2001[982] restricts the connection of telephone analysers to a telecommunications network for this purpose; however, those provisions would not apply in this scenario where the call data is obtained without the attachment of any device to the network. The wife could make a complaint to the Privacy Commissioner under principle 4; however, the husband may be able to rely on the domestic affairs exception in section 56 of the Privacy Act.

Scenario 13: vehicle tracking

9.112 ***J** is the television personality from Scenario 6 who is rumoured to be a drug addict. A journalist arranges for a tracking device to be installed in **J**'s car by a private investigator. A log of the car's movements is then compiled, based on data from the tracking device. The data confirms that the car regularly visits a drug rehabilitation clinic in another town. The journalist places the clinic under visual surveillance, and captures pictures of **J** entering and leaving the clinic, which are then published in a national newspaper.*

9.113 If a Police officer wanted to place a tracking device on **J**'s car as part of an investigation into a possible drug offence (for example), he or she would have to apply for a warrant in most circumstances.[983] However, there is no complementary criminal offence, and tort liability is uncertain. Neither the journalist nor the private investigator has committed a criminal offence in using the tracking device. The attachment of the tracking device to **J**'s car may amount to a trespass to goods for which **J** could sue.

980 Certain spyware is capable of intercepting calls, as well as converting the cell-phone into a listening device: see Bob Segall "Tapping Your Cell Phone" (14 November 2008) www.wthr.com (accessed 14 December 2008).

981 Judge David Harvey *Internet.law.nz: Selected Issues* (2 ed, LexisNexis, Wellington, 2005) 210.

982 Telecommunications Act 2001, ss 106-111.

983 Summary Proceedings Act 1957, ss 200A-200P; see also Search and Surveillance Powers Bill 2008, no 300-1, cl 46(a).

9.114 The Privacy Act would not apply to the actions of the journalist if the journalist's activities are "news activities", but the Privacy Act principles would apply to the actions of the private investigator in compiling the log of **J**'s movements. If this is unfair or intrudes to an unreasonable extent upon **J**'s personal affairs, it may breach principle 4.

9.115 The Press Council privacy principle may not apply if there is "significant public interest" in the story. The publication of the photographs showing that **J** attends a rehabilitation clinic may be actionable under the privacy tort for publication of private facts, although the newspaper could use the defence of legitimate public concern in the story.

Scenario 14: workplace tracking

9.116 *A telecommunications company proposes to install GPS in field employee work vehicles. The GPS would be used to increase dispatch efficiency, manage assets and reduce mileage and fuel consumption. Information on the start and stop times of vehicles and their locations would be used in capacity planning, productivity analysis and performance management, as required. The company's GPS policy outlines what information would be collected, the purposes of the collection and the personnel who would have access to the information. Several employees complain that the company will be improperly collecting their personal information.*[984]

9.117 It is not an offence to use or install tracking technology, regardless of whether or not the consent of the person being tracked has been obtained. The Privacy Act would likely permit the collection of GPS information from the company's vehicles as the purposes for collecting the information are lawful and the information is necessary to achieve those purposes. Principle 3 would require the company to give adequate notice to the employees, which it could do by circulation of the company's policy on GPS information. The company would also have to comply with the other privacy principles, including principle 10's requirement that the information not be used for purposes other than those for which it was obtained. In addition, the company would have to comply with employment law principles such as trust and good faith, and with procedural fairness requirements if information from the GPS was used to discipline or dismiss a worker (see chapter 12).

Scenario 15: computer spyware (i)

9.118 *A woman purchases software which remotely collects data from computer hard drives. The woman installs this software on a friend's computer, without his consent, and uses the software to record her friend's online activities, including his login details for online banking. Although the software program is used to collect and return this information to the woman, she does not use the information to withdraw money from her friend's account.*[985]

---

984 This scenario is based on the facts of a complaint to the Office of the Privacy Commissioner of Canada, *Use of Personal Information Collected By Global Positioning System Considered* (PIPEDA Case Summary #351, 2006). The Assistant Privacy Commissioner concluded that the use of GPS was for acceptable purposes and, because the company took measures to limit its use for employee management, it could also be used for that purpose in certain circumstances.

985 This scenario is taken from the Australian Government, Department of Communications, Information Technology and the Arts *Spyware Discussion Paper* (May-June 2005) 14.

9.119 The installation of the spyware is likely to give rise to one or more of the computer misuse offences under sections 249 or 250 of the Crimes Act. The friend could make a complaint to the Privacy Commissioner that there has been an unlawful or unreasonable intrusion into his personal affairs in breach of principle 4. However, section 56 (the collection of personal information for a personal affairs purpose) could exempt any breach of the privacy principles, particularly if the two friends lived together in the same household.

Scenario 16: computer spyware (ii)

9.120 *A journalist seeking information about the subject of a corruption investigation sends a Trojan horse email to the subject of the investigation that, when opened by the recipient, copies all data on the subject's hard drive (including copies of all incoming and outgoing emails) and relays it to an email account that cannot be traced back to the reporter.*[986]

9.121 The Trojan Horse email is likely to give rise to at least one of the computer misuse offences, either under section 249 of the Crimes Act (given the reasonably broad concept of "benefit" in the case law) or under section 250 of the Crimes Act (given the reasonably broad concept of "damage" in the case law). In relation to the emails, the interception offence would not apply if the emails are copied on receipt by the recipient's computer (rather than in transit). In any event, the definition of interception device anticipates some sort of tangible device and may not be broad enough to include computer software.

9.122 The Privacy Act will not apply if the journalist's activities are "news activities". Otherwise, the owner of the emails could bring a privacy complaint to the Privacy Commissioner for breach of principle 4. The person affected could make a Press Council complaint on publication of any story based on the emails, but the Press Council privacy principle may not apply if there is "significant public interest" in the story.

CONCLUSION

9.123 In this chapter we have summarised the laws currently applying to surveillance. They are patchy and without much coherence. The scenarios we have presented demonstrate some of the difficulties. In some situations there are several alternative remedies and sanctions available. In others there are remedies or sanctions not for the surveillance itself, but for subsequent inappropriate use of the recordings or information obtained. In yet other situations there seem to be no clear remedies or sanctions at all, unless one is prepared to stretch or expand ones designed for other purposes. Throughout there is a mix of criminal sanctions, civil remedies and regulatory controls. In the next chapter, we shall explore whether, and if so how, the law needs to be improved.

986 Based on an example cited by Nick Davies *Flat Earth News: An Award-Winning Reporter Exposes Falsehood, Distortion and Propaganda in the Global Media* (Chatto & Windus, London, 2008) 278. See also the discussion of mirror walls that allow the copying of email traffic. For a description of the Trojan Horse program "Back Orifice" see *R v Garrett* [2001] DCR 955, para 14.

Chapter 10

Reform of the law on surveillance

10.1 In this chapter we consider possible reforms of the law. We consider a number of options. In deciding what might best be done we need to weigh a number of factors.

10.2 The *location* where the surveillance is undertaken is relevant. When people are in their own homes, they have a strong expectation of privacy, so that they may conduct themselves as they please without the inhibition of knowing or suspecting that they are being watched. When they are in their backyards there is a greater chance that they will be observed, but even there they have some expectation of privacy. When they are in public places or places to which the public has access, where they can be seen by anyone who is there, their expectations of privacy are greatly reduced.

10.3 However, location is not the sole determinant. The *nature* of the act of surveillance, and the *purpose* of the person undertaking it, are relevant as well. "Up-skirt" filming is objectionable even if done in a public place. It may also be objectionable to film a person in a particularly vulnerable situation, such as after a serious accident.

10.4 Subsequent *use* of the information obtained is important. Even if the act of surveillance is itself unobjectionable, as CCTV surveillance may often be, people still have a right to be concerned about the uses to which the images obtained might be put. It is one thing for the Police, or a mall owner, to use images for the purposes of crime detection. It is another altogether for embarrassing images of a person captured in CCTV footage to be published on the internet. The use, and security, of the information obtained by surveillance is often of more concern than the surveillance itself.

10.5 *Covert* surveillance, of which the subject is unaware, is generally of more concern than *overt* surveillance which the subject is aware of. If people know, or suspect, that they are being watched, they have an opportunity to modify their conduct. The BSA draws this distinction when it applies its intrusion principle. However, as we indicated in chapter 8, the line between overt and covert surveillance is not always a clear one, and overt surveillance can also have significant negative effects.

10.6 The monitoring and recording of private conversations is often of more concern than the taking of visual images. *Listening* can, in many cases, convey more information than *looking* at pictures. Moreover, listening to a private conversation is more destructive of relationships, and more inhibiting to freedom of expression and information. Thus, even monitoring private conversations in a public place by means of long-range microphones or other devices is usually unacceptable. Again, however, the line is not a clear one: much can be learned about people's feelings, activities and relationships by watching them, too.

10.7 As indicated above, *purpose* is always important. Surveillance for voyeuristic purposes is a very different thing from surveillance for law enforcement purposes. It will thus be important either to define the ingredients of the various prohibitions precisely, or to provide specifically for defences and exceptions to them. That is currently done in the Privacy Act, and in criminal provisions such as the intimate covert filming offences in the Crimes Act.

CIVIL LAW REFORM OPTIONS

10.8 None of the existing civil remedies deal with the intrusion of surveillance either comprehensively or particularly clearly. Potential civil law reform options include:

- The use of surveillance devices in certain circumstances could give rise to civil liability under a general statutory privacy tort, an intrusion tort or a specific surveillance tort.
- Where criminal offences are created against the covert use of surveillance devices, corresponding civil liability could be confirmed by statute.

10.9 We do not raise breach of confidence as a reform option. In *Hosking v Runting*, the New Zealand Court of Appeal (by a majority) has not relied on the doctrine of breach of confidence in the context of disclosure of private information, but rather has preferred to name the relevant cause of action as one in privacy.[987] Relying on breach of confidence in the context of surveillance may not be consistent with this development of the privacy tort and may make it more difficult to establish a coherent privacy framework.

10.10 In selecting a preferred framework for civil liability, one factor to consider will be the relationship between the criminal and civil law. A framework for civil liability based on breach of statutory duty would be fairly consistent with the criminal law framework (based on either a generic or targeted approach discussed further below). Other tort options could either be broader than the criminal law or fairly consistent with it, depending on the criminal law approach selected.

Privacy, intrusion or surveillance tort

10.11 One option is the creation of a general statutory privacy tort or statutory intrusion tort that could give rise to civil remedies for intrusions into privacy caused by activities such as covert or targeted surveillance. The criteria for such a tort would need to be carefully formulated to ensure that it is tightly confined. It should be limited to situations where the intrusion is objectionable, in circumstances where the plaintiff has a reasonable expectation of privacy.

987 *Hosking v Runting* [2005] 1 NZLR 1 para 45 (CA) Gault P and Blanchard J: "Privacy and confidence are different concepts. To press every case calling for a remedy for unwarranted exposure of information about the private lives of individuals into a cause of action having as its foundation trust and confidence will be to confuse those concepts."

There should be a defence of public concern. Statutory privacy torts in four Canadian provinces list certain acts of surveillance as examples of privacy intrusions that are covered by the tort.[988] A statutory cause of action for invasion of privacy is also under consideration at the Federal level in Australia. The proposal is that the cause of action would include a non-exhaustive list of the types of privacy invasions covered, including unauthorised surveillance.[989] The issues associated with a possible intrusion tort are discussed in chapter 11.

10.12 An alternative to a general privacy tort or an intrusion tort would be to create a more specific statutory tort against privacy-invasive surveillance. A surveillance tort may have clearer boundaries that a more general intrusion tort. The Irish Law Reform Commission recommended a specific surveillance tort that would operate in circumstances where a person has a reasonable expectation of privacy, the privacy expectation to be determined on the basis of a number of factors including the place where the surveillance occurred (private or public), the object of the surveillance (whether intruding into private life), the use to which the material obtained was to be put (objectionable or innocuous), and the means of surveillance used (natural senses or the use of a surveillance device), allowing the courts to interpret the extent of the right of privacy in each case.[990] However, the Commission's recommendation has not been implemented in Ireland. A surveillance device tort was also proposed in the United Kingdom by the Younger Committee;[991] however, that proposal was not taken up by the British government.

10.13 An example of a statutory surveillance device tort can be found in the California Civil Code:[992]

> A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.

988 Privacy Act CCSM s P125 (Manitoba) s 3; Privacy Act 1990 RSNL c P-22 (Newfoundland and Labrador) s 4; Privacy Act 1978 RSS c P-24 (Saskatchewan) s 3; Privacy Act 1996 RSBC c 373 (British Columbia) s 1(4). These include auditory or visual surveillance, and listening to or recording someone's conversations. The British Columbia Law Institute has recently recommended adding unauthorised monitoring of a computer or electronic device as an additional deemed privacy violation: *Report on the Privacy Act of British Columbia* (BCLI R49, Vancouver, 2008) recommendation 2.

989 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 74-1.

990 Law Reform Commission of Ireland *Privacy: Surveillance and Interception of Communications* (LRC 57-1998 Dublin) paras 7.04-7.08.

991 Rt Hon Kenneth Younger *Report of Committee on Privacy* (Cmnd 5012, London, 1972) para 565.

992 California Civil Code, s 1708.8(b). There is also civil liability for physical invasion of privacy involving trespass under s 1708.8(a), and civil liability if a person directs or induces a physical or constructive invasion of privacy by another person under s 1708.08(e). There is an exception for law enforcement officers and others who use surveillance in the course of their employment to obtain evidence of illegal or fraudulent conduct under s 1708.8(g).

10.14 Some of the issues that are raised in relation to an intrusion tort in chapter 11 would also be relevant to consideration of a surveillance tort, such as the defence of legitimate public concern, as well as other defences and remedies.

10.15 In chapter 11 we raise questions about parameters of an intrusion tort and whether it should be limited to "solitude and seclusion" or apply more broadly whenever someone has a reasonable expectation of privacy, including in public places. Nicole Moreham, for example, has suggested people should be presumed to have a reasonable expectation of privacy if they are involuntarily experiencing an intimate or traumatic experience (such as being extricated from a car accident), are in a place where they might reasonably believe they are imperceptible to others (in remote secluded places), or if technological devices are used to intrude into their personal zone (such as an x-ray device to see through clothing, or a shotgun microphone to listen to private conversations). Taking a photograph or making some other kind of record in these situations, she suggests, should give rise to civil liability. There would need to be public interest defences which would cover such matters as law enforcement and newsgathering.[993] The British Columbia Law Institute has recently recommended that the statutory tort in that province provide that a person may expect a reasonable degree of privacy with respect to lawful activities in a public setting which are not directed at attracting publicity or the attention of others.[994]

10.16 The United States intrusion tort, although generally covering intrusions into a private place or private seclusion, also extends to intrusions in public places in certain circumstances. In *Galella v Onassis*,[995] the intrusion tort was invoked to restrain a journalist whose following and photographing of Jacquie Onassis and her children in public amounted to harassment. The tort has also been invoked to restrain photographs of people in "involuntary" embarrassing situations in public places. In *Daily Times Democrat v Graham*, a photographer who photographed a woman whose skirt was blown up by a jet of compressed air at a "Fun House" was found to have invaded her privacy.[996]

> Q33 Should civil liability for certain uses of surveillance devices be provided for by means of a statutory privacy tort or intrusion tort (as discussed in chapter 11), or a statutory surveillance tort? If so, what uses of surveillance devices should the tort cover?

Breach of statutory duty

10.17 In chapter 2 we noted the tort of breach of statutory duty and its inherent uncertainty. One option for reform would involve clarification through new statutory provisions that use of a surveillance device in certain circumstances may give rise not only to criminal prosecution, but also to civil liability.

993 NA Moreham "Privacy in Public Places" (2006) 65 CLJ 606, 634-635.

994 British Columbia Law Institute *Report on the Privacy Act of British Columbia* (BCLI R49, Vancouver, 2008) recommendation 3.

995 *Galella v Onassis* (1973) 487 F 2d 986 (2nd Cir).

996 *Daily Times Democrat v Graham* (1964) 276 Ala 380. However, the tort did not apply where a picture of a football player was taken with his consent but without his knowledge that his fly was open: *Neff v Time, Inc.* (1976) 406 F Supp 858.

This option would afford a degree of consistency between the criminal and civil law, as well as removing the need for argument as to whether the tort was available in relation to those provisions. Consideration would need in each instance to be given to whether or not the correspondence between the civil and criminal liabilities was to be exact: whether, for example, the same defences applied.

10.18 It is worth noting that some offences that afford privacy protection (such as the computer misuse offences) have a broader rationale than privacy protection. Civil liability triggered by breach of these offences would therefore likely extend beyond the privacy context.

Q34 Should civil liability for the use of surveillance devices be based on breach of a statutory duty?

Harassment Act

10.19 For surveillance that is harassing or intimidating, one option may be to amend the Harassment Act to include certain acts of surveillance as "specified acts" of harassment. The Harassment Act does not deal specifically with the use of surveillance devices to harass and intimidate. The Act is triggered where there is a pattern of behaviour (at least two specified acts of harassment in a 12-month period). As we discussed in chapter 9, it could be difficult to apply this requirement for two or more separate acts to continuous surveillance. There may therefore be a case for providing in the Harassment Act that certain acts of surveillance using surveillance devices would be acts of harassment on their own, without requiring any further harassing act to occur. This would allow the subject of the surveillance to apply for a restraining order upon being subjected to an act of surveillance. Consideration might also be given to amending the Act to allow for a damages remedy in certain circumstances, a matter which we return to in chapter 11. Where such surveillance also causes the subject to fear for his or her safety, this could constitute an act of criminal harassment. The "lawful purpose" defence in section 17 of the Act would continue to apply.

Q35 Should certain targeted surveillance activities be designated "specified acts" of harassment under the Harassment Act?

Q36 Should certain acts of surveillance be considered to constitute harassment on their own, without a requirement for any further specified act directed at the applicant to occur, for the purposes of seeking a restraining order or bringing a criminal charge under the Harassment Act 1997?

CRIMINAL LAW REFORM OPTIONS

10.20 As we saw in the last chapter, there are a number of specific offences targeting various types of surveillance activity. There are also some summary offences, broadly framed ("peeping and peering" and offensive behaviour, for example), which can be used to catch various manifestations of surveillance activity. The specific offences largely deal with the use of particular categories of devices, such as visual surveillance or interception devices. The relevant summary offences are generic. We consider now some possible models for reform.

Location

10.21 The place where the surveillance takes place will be relevant in the formulation of any criminal offences. In some places (a dwellinghouse, for instance) there is a much stronger privacy interest than in others (public places, or places like shopping centres to which the public has access). The location of a privacy intrusion by surveillance will thus often be an indicator of the significance of the intrusion. In particular, visual surveillance of private property is generally a significant intrusion, although visual surveillance can sometimes also be intrusive in other places. Communications privacy is significant in private environments (particularly oral communications in private); however, the expectation as to communications privacy is not limited to private environments, as the mobility of communications technology has expanded the range of locations in which private communications take place. The location of an intrusion is not a factor for location privacy (tracking someone's movements in a range of locations), or data privacy.

10.22 In some jurisdictions offence provisions have been proposed that specifically target surveillance intrusions into private places. Offences have been recommended against the use of a surveillance device in relation to a private dwelling (Ireland)[997] or private premises (Hong Kong)[998] that infringes a person's privacy; or on private property, or in relation to a person who is on private property, with intent to obtain personal information (National Heritage Committee).[999] In each case a number of defences were proposed, some having a public interest component such as preventing the public from being misled by a public statement, informing the public about the discharge of public functions and the protection of health and safety.[1000] None of these proposals, however, have been implemented.

997 Law Reform Commission of Ireland *Privacy: Surveillance and the Interception of Communications* (LRC 57-1998, Dublin) para 9.07.

998 Hong Kong Law Reform Commission *Privacy: the Regulation of Covert Surveillance* (Hong Kong, 2006) para 1.33.

999 National Heritage Committee *Privacy and Media Intrusions* (Fourth Report, vol. 1, March 1993) para 52. The Government response accepted the principle that certain forms of intrusion should be subject to the criminal law; however it identified the key problem as coming up with an acceptable legislative formula that adequately addressed the mischiefs in question and yet combined clarity with sufficient sensitivity to the legitimate pursuit of investigative journalism: *The Government's Response to the House of Commons National Heritage Select Committee: Privacy and Media Intrusion* (Cmnd. 2918, 1995).

1000 National Heritage Committee *Privacy and Media Intrusions* (Fourth Report, vol. 1, March 1993) para 55.

10.23 Both the Irish and Hong Kong Law Reform Commissions also proposed new criminal offences targeting surveillance involving trespass: trespass on private property for the purpose of surveillance (Ireland),[1001] and entering or remaining on private premises as a trespasser with intent to observe, overhear or obtain personal information (Hong Kong).[1002] The National Heritage Committee proposed an offence of entering private property without the consent of the lawful occupant, with intent to obtain personal information. The proposed offences were also to be subject to various defences, but have not been enacted.

Generic or specific?

Generic

10.24 From time to time options for criminal offences relating to surveillance have been proposed which are generic, that is to say, not dependent on the type of surveillance device used. In other words, such a crime would be constituted by any type of surveillance, be it audio, visual or of any other kind.

10.25 A generic approach for the criminal law was suggested in the 1970s by the Younger Committee, which proposed an offence of surreptitious surveillance (by use of a surveillance device).[1003] The approach was suggested more recently by the New South Wales Law Reform Commission, defining surveillance as:[1004]

> The use of a surveillance device in circumstances where there is a deliberate intention to monitor a person, a group of people, a place or an object for the purpose of obtaining information about a person who is the subject of the surveillance.

Under the proposed regime, all covert use of surveillance devices would be prohibited without prior independent authorisation (such as a warrant). This proposed regime was not implemented and New South Wales has since enacted the Surveillance Devices Act 2007 (NSW), an example of a more specific approach.

10.26 The advantage of a generic approach is that it would provide protection under the criminal law against surveillance from new technologies as they arise. There is always a difficulty where the law trails technology.[1005] One way for the law to keep up with technological challenges is to craft a more generic offence that will not become obsolete as technology changes.

1001 Law Reform Commission of Ireland *Privacy: Surveillance and the Interception of Communications* (LRC 57-1998, Dublin) para 9.10.

1002 Hong Kong Law Reform Commission *Privacy: the Regulation of Covert Surveillance* (Hong Kong, 2006) para 1.12.

1003 Rt Hon Kenneth Younger *Report of Committee on Privacy* (Cmnd 5012, London, 1972). For elements of the offence, see para 563.

1004 New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC R98, Sydney, 2001) recommendation 2.

1005 See for example the opinion of Bruce Schneier "Schneier on Privacy (and the Lack Thereof)" (5 November 2008) http://blogs.cioinsight.com (accessed 10 November 2008).

10.27 However, there are difficulties with applying a generic approach in the criminal law. The criminal law needs to be precise. The criminal law also tends to target behaviours of particular seriousness.[1006] Any generic approach would require at least some limitation: one such limitation might be that it applied only to covert surveillance. Yet, as we have seen, the line between covert and overt surveillance is often far from clear. Even if the line were clear, most would say that not all forms of covert surveillance are sufficiently serious to justify the intervention of the criminal law. The level of seriousness or intrusiveness turns on a number of factual variables such as the type of surveillance, the place where the surveillance occurs (public or private), the type of device used, the purpose for which the device is used, the use to which any information obtained will be put, the nature of the activity being observed (intimate activity, other private activity, or non-private activity) and whether there are any overriding public interest factors. Any generic offence may need to include a list of factors to be assessed by the presiding judge, as well as some sort of threshold (such as offensive or highly offensive to a reasonable person) and possibly a public interest defence, so that the offence is not overbroad.

Specific

10.28 We prefer any provisions creating criminal liability to be specific, and in particular to be directed at defined uses of certain types of surveillance device. Thus, there might be provisions dealing with visual surveillance, interception, tracking or data monitoring or specific technologies (such as RFID).

10.29 Such an approach is taken in the Surveillance Devices Acts enacted in various states or territories of Australia. These Acts prohibit certain uses of:

- visual surveillance devices to observe and record private activity (or uses that involve a form of trespass);
- listening devices to record private conversations;
- tracking devices to determine a person's location without consent; and
- data surveillance devices.

10.30 While containing general prohibitions on particular uses of devices, these Acts nevertheless permit such uses in certain circumstances. For example, the Surveillance Devices Act 1998 (WA) allows for the use of listening devices and optical surveillance devices in the "public interest", defined to include:[1007]

> the interests of national security, public safety, the economic wellbeing of Australia, the protection of public health and morals, and the protection of the rights and freedoms of citizens.

10.31 Generally, the publication of material obtained from the illegal use of listening and optical surveillance devices is unlawful. However, provision is made for publication in certain circumstances. For example, the Western Australian Act makes provision for a judge to allow publication of material obtained from illegal surveillance in the public interest.[1008]

1006 See discussion of the role of the criminal law in chapter 5.

1007 Surveillance Devices Act 1998 (WA), s 24.

1008 Surveillance Devices Act 1998 (WA), s 31. The Surveillance Devices Act 1999 (Vic), s 11, also allows for the publication of material obtained from the illegal use of surveillance devices in the public interest.

10.32 The difficulty with this approach is that it may be more difficult to achieve consistency between the various offences, and it may not sufficiently take account of future developments, thus requiring regular updates and amendments.[1009] A specific approach may therefore lack the flexibility to apply to new surveillance devices or techniques as they are developed, without statutory amendment or supplementation.

10.33 Nevertheless, at this initial stage of our Review, we tend to prefer a more specific approach as the primary basis for developing criminal law responses to surveillance. Such an approach would build on the existing criminal law; would complement the surveillance device warrant regime proposed in the Search and Surveillance Powers Bill 2008 (which is based on the functional use of surveillance devices to intercept, watch and track); and would be consistent with the development of the criminal law in Australia. A specific approach proscribing uses of surveillance devices in particular circumstances would have more clearly-defined parameters and may have the advantage of greater certainty as to when surveillance offences would apply.

Q37 Should the use of surveillance devices continue to be dealt with under the criminal law by targeting specific uses of surveillance devices in particular circumstances? Alternatively, should these offences be dealt with more generically? If so, how could this be achieved?

SPECIFIC CRIMINAL LAW REFORM OPTIONS

Watching and visual recording

Visual surveillance device offence

10.34 There is currently no offence in New Zealand of using a surveillance device to record a private activity, unless it comes within the definition of intimate covert filming in the Crimes Act 1961. However the Law Commission, in its report on *Search and Surveillance Powers*, had cause to consider the acceptable boundaries of such conduct. The Search and Surveillance Powers Bill 2008, which followed from the Commission's report, proposes that law enforcement agencies should obtain a surveillance warrant to use visual surveillance devices to observe private activity in a private building and, if the surveillance continues for longer than a specified period, in the curtilage of such a building.[1010] The activity under surveillance is "private activity" if any participant ought reasonably to expect that it is observed or recorded by no one except the participants.[1011] This will depend on the privacy of the location; for example, whether the location is observable by anyone passing or living nearby. Activity that is observable without trespass and without the use of a visual surveillance device will probably not be private activity.[1012]

1009 See New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007) para 11.3.

1010 Search and Surveillance Powers Bill 2008, no 300-1, cl 46(b) and (c).

1011 Search and Surveillance Powers Bill 2008, no 300-1, cl 3.

1012 See Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (The Federation Press, Sydney, 2005) 145.

10.35 The question is whether any activities of the kind for which law enforcement agencies will require a warrant under the Bill's provisions should be an offence if undertaken by other persons, or indeed by anyone without a warrant.

10.36 In creating any new offence, the following issues would need to be considered:

- Whether any offence should be confined to cases where a trespass has taken place, or should be more general.
- Whether visual surveillance should include both watching (such as using telescopes and binoculars) and recording (such as using video cameras), or should be limited only to recording.
- Whether a distinction should be made between overt and covert visual surveillance.
- Besides a warrant exception for law enforcement officers, whether there should be any defence to a visual surveillance offence on grounds of public interest; who would be entitled to use any such defence; and where the limits of the defence might lie.[1013]
- How visual surveillance by property owners of their own properties (for example, for security purposes) could be accommodated while limiting invasions of the privacy of people present at the property.[1014]
- How visual surveillance in the workplace should be dealt with.[1015]

10.37 If the Search and Surveillance Powers Bill 2008 is enacted, it will follow that activities for which law enforcement agencies do not need a warrant will generally be lawful by whomsoever they are undertaken. However, the Commission would be interested in views as to whether there may be circumstances in which, or purposes for which, visual surveillance ought to be criminal even though:

- it is of private activity in other than a private building or its curtilage; or
- it is of "non-private" activity in a private building.

10.38 In Australia several states have enacted offences against the use of optical surveillance devices:

- In Victoria and the Northern Territory, it is an offence to use optical surveillance devices to record a private activity.[1016]
- In Western Australia, it is an offence to use optical surveillance devices to observe or record a private activity.[1017]

These offences regulate the visual surveillance of private activity but do not prohibit the visual surveillance of "non-private" activity in private homes.

1013 See, for example, the growing use of video cameras and cell-phone cameras by private citizens to capture visual evidence of criminal offending that can be passed on to the police: "Video Cameras Silence Hoons" (8 May 2008) www.stuff.co.nz (accessed 12 May 2008); Andrew Charlesworth "Public Urged to Record Crime with Cameraphones" (1 June 2007) www.vunet.com (accessed 28 October 2008).

1014 One possibility is that this sort of surveillance could generally be required to be overt by the giving of notice of the surveillance.

1015 See chapter 12 below.

1016 Surveillance Devices Act 1999 (Vic), s 7(1); Surveillance Devices Act 2007 (NT), s 12(1).

1017 Surveillance Devices Act 1998 (WA), s 6(1).

10.39 A different formulation is used in New South Wales, where it is an offence to use optical surveillance devices on or within premises or vehicles, or on any other object, to record or observe any activity if the use of the device involves trespass to land or trespass to goods (that is, entry to premises or a vehicle without consent, or interference with a vehicle or other object without consent).[1018] The offence therefore does not restrict visual surveillance of one's own property, although the Workplace Surveillance Act 2005 (NSW) will apply to visual surveillance in workplaces.

Visual surveillance in public places

10.40 Visual surveillance in a public place should be an offence only in a limited range of circumstances where the conduct of the person undertaking the surveillance is particularly offensive, or done with improper motives which are serious enough to warrant the intervention of the law. "Up-skirt" filming, already an offence, is an illustration, as is persistent conduct amounting to criminal harassment under the Harassment Act 1997.

10.41 The summary offence of offensive behaviour in a public place[1019] has been employed to deal with surreptitious photography, although the two *Rowe* cases illustrate that covert photography does not easily fall under the offence.[1020] It depends on the conduct being such that it would be considered offensive by a reasonable observer. There may be problems where the covert behaviour is not observed by anyone and is only discovered later. Another issue is where the observable behaviour is not sufficiently offensive without reference to the surrounding circumstances such as the person's motive and pattern of behaviour, and the use to which the photographs will be put. The taking of one surreptitious photograph on its own may not be offensive, but may be offensive if placed in the context of other behaviour such as a collection of photographs that objectify the subjects. The offence is only indirectly protective of privacy. This is because the offensiveness test is applied from the perspective of a reasonable person in the position of a person *witnessing* the behaviour, regardless of whether or not that person is the *target* of the behaviour.[1021] The Supreme Court has likewise held that, insofar as the same section of the Summary Offences Act proscribes "disorderly" behaviour, its purpose is not the protection of privacy.[1022]

10.42 The question is whether any more satisfactory mechanism is needed to control privacy-intrusive photography in a public place and, if so, whether one can be devised. Possible options would be to modify the offensive behaviour offence to better take account of privacy-intrusive surveillance, or to develop a new offence for this purpose. Any such offence would have to be carefully defined.

1018 Surveillance Devices Act 2007 (NSW), s 8.

1019 Summary Offences Act 1981, s 4.

1020 See also Alisdair A. Gillespie "'Up-Skirts' and 'Down Blouses': Voyeurism and the Law" [2008] Crim LR 370, 372-377 for discussion of problems with prosecuting objectionable photography under the English common law offence of outraging public decency.

1021 Cf the "highly offensive" element of the tort of publication of private facts, which is applied from the position of the person affected by the disclosure: see para 6.60 above.

1022 *Brooker v Police* [2007] 3 NZLR 91.

Hidden cameras

10.43 Consideration could be given to whether a more specific offence against the use of hidden cameras would be desirable, either in private places or generally, subject to a public interest defence. In the United States, 13 states expressly prohibit the unauthorised installation or use of hidden cameras in private places (places where a person may reasonably expect to be safe from unauthorised surveillance).[1023]

Intimate visual recording

10.44 Intimate visual recording applies to the covert use of visual surveillance devices to record intimate material, largely in private places, although the up-skirt filming offence applies to the capturing of intimate images from under a person's clothing where the person is in a public place as well. It has been suggested that the wording of the up-skirt filming offence:[1024]

> Encompasses both cases where the person making the recording has concealed the relevant equipment beneath or under his or her clothing and other cases where a device not necessarily so concealed is recording images of the parts of the subject person's body through or under the subject's clothing.

The policy intent of the up-skirting offence, however, is clearly only the latter case.[1025] If the intimate visual recording offence is to include covert intimate filming in public places other than up-skirt filming (for example, surreptitious photography of topless sunbathers), this may require legislative amendment.

10.45 The intimate covert filming provisions of the Crimes Act also do not cover situations in which an intimate visual recording is made with consent, but is subsequently published or distributed without consent. This is consistent with the policy intent of the offence.[1026] We raised in chapter 7 the question of whether additional criminal offences are required for particularly serious disclosures of personal information (including intimate images) without consent.

Q38 Are any reforms to the criminal law relating to visual surveillance required, such as:

- a new visual surveillance device offence;
- reform of the summary offence for offensive behaviour in a public place or a new offence to cover intrusive visual surveillance in public;
- an offence against the use of hidden cameras; or
- expansion of the intimate visual recording offence?

1023 Alabama, Arkansas, California, Delaware, Georgia, Hawaii, Kansas, Maine, Michigan, Minnesota, New Hampshire, South Dakota, and Utah: Greg P Leslie (ed) *The First Amendment Handbook* (The Reporters Committee for Freedom of the Press, 2003) www.rcfp.org (accessed 20 October 2008).

1024 Hon Bruce Robertson (ed) *Adams on Criminal Law* (loose leaf, Brookers, Wellington, Crimes Act, 1992) para CA216G.03 (last updated 30 March 2007).

1025 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) para 4.16, makes it clear that what is targeted is covert filming under the *subject*'s clothing; see also para 4.65, noting that covert intimate filming in public places such as secret filming of topless bathing on a public beach is not covered by the scope of the intimate visual recording offences.

1026 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) para 4.65.

Q39 Should any of these matters concerning visual surveillance be dealt with instead by way of civil liability (under a tort or the Privacy Act)?

Q40 What should be the scope of any new visual surveillance offences?

Listening and interception

10.46 The covert interception of private communications between people (which includes listening and recording their conversations) can in many cases be more intrusive of privacy than visual surveillance of them. Recording the conversation of two people usually provides more information about them than their visual images (although pictures can also tell us something about a person's relationships and activities). Thus, we tend to find the secret recording of a private conversation in a public place more objectionable than a photograph taken there.

Private communications

10.47 The definition of "private communication" for purposes of the interception offence in section 216A of the Crimes Act 1961 is not straightforward. Its meaning was considered in *Moreton v Police*,[1027] where the Judge noted that the definition has both an inclusive part and an exclusive part:

- It includes 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.[1028]
- It excludes a communication if the parties ought reasonably to expect that the communication may be intercepted by a person who does not have the consent of a party.[1029] If one party ought reasonably to expect that the communication might be intercepted, this does not render the communication non-private unless the other parties also ought to have had the same expectation.[1030]
- This means, as the judge conceded, that the words "any party" have different senses in the inclusive and the exclusive parts: they mean "one or more parties" in the first, but "all parties" in the second.

10.48 The case also considered what sort of expectation is necessary to exclude a communication from being private, one of the questions being whether a person using a cellphone or portable phone ought reasonably to expect that the call may be intercepted. Acknowledging that most people who use cellphones recognise that these phones are not secure and may conceivably be intercepted, the Judge concluded that the likelihood of interception must be assessed:[1031]

1027 *Moreton v Police* [2002] 2 NZLR 234 (HC) William Young J.

1028 Crimes Act 1961, s 216A(1)(a) (definition of "private communication").

1029 Crimes Act 1961, s 216A(1)(b) (definition of "private communication"). For example, listening to a conversation on a CB radio or the use of a scanner to listen to emergency services and police frequencies would not be offences as no one could reasonably expect the communications to be confined to the parties: Judge David Harvey *Internet.law.nz: Selected Issues* (2 ed, LexisNexis, Wellington, 2005) 239.

1030 *Moreton v Police* [2002] 2 NZLR 234 (HC) William Young J.

1031 *Moreton v Police* [2002] 2 NZLR 234 para 70 (HC) William Young J.

> My impression as an ordinary cellphone-using member of the community is that while I recognise that cellphone calls can be intercepted, I do not have an expectation that this is particularly likely in relation to any particular call which I might make.

The Judge considered that there were a number of issues that warrant legislative consideration, including whether the definition of "private communication" should be left in its present form given its potential for ambulatory application as public expectations as to the likelihood of interception change over time.[1032]

10.49 Judge Harvey in his book also raises questions about the strength of the privacy expectation necessary for a communication to qualify as a private communication, such as whether cellphone communications and unencrypted email qualify as private communications.[1033]

10.50 The law reform question is whether the definition of "private communication" should be clarified or simplified. One option might be to limit the application of the exclusive part of the definition only to certain forms of communication and to remove it for other forms of communication. While the exclusive part may be necessary in relation to the interception of face-to-face communications so that the offence is not overbroad (for example, to avoid limiting the use of tape recorders at lectures or public meetings), and in relation to communications by CB radio which are wholly unsecure, there is a question as to whether it should be applied in relation to telephone calls, text messages and emails. The alternative option is that these forms of communication could simply be presumed to be private for the purposes of the interception offence, regardless of the likelihood of interception.

10.51 The prohibition on interception in the Australian Telecommunications (Interception and Access) Act 1979 for example, prohibits third parties from intercepting a communication passing over a telecommunications system, without the knowledge of the person making the communication.[1034] In another example, the California Penal Code definition of "confidential communication" (the equivalent of "private communication") has the same excluding part for the purposes of the offence of eavesdropping or recording a communication,[1035] but there are separate offences for the interception of communications transmitted between cellphones and landline telephones,[1036] between cordless phones, landline telephones

1032 *Moreton v Police* [2002] 2 NZLR 234 paras 22-23, 36 (HC) William Young J.

1033 Judge David Harvey *Internet.law.nz: Selected Issues* (2 ed, LexisNexis, Wellington, 2005) para 4.9.3.

1034 Telecommunications (Interception and Access) Act 1979 (Cth), ss 6(1) and 7(1). See Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (The Federation Press, Sydney, 2005) 142. At state level, the various interception offences operate in a similar way to the New Zealand offence (although the exclusive part of the definition of "private conversation" is not used in the Listening And Surveillance Devices Act 1972 (SA)). It is also worth noting that the offences at state level all deal only with listening devices, while the New Zealand offence deals with a broader range of interception devices.

1035 California Penal Code, s 632(c): "The term 'confidential communication' includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded."

1036 California Penal Code, s 632.5.

and cellphones,[1037] and for the interception and recording of any communication between cellphones, landline telephones and cordless telephones,[1038] that do not rely on the definition of "confidential communication."

10.52 A comparison could also be made to the computer misuse offences,[1039] where there is no exception for accessing unsecure systems (although there is an exception to one of the offences for unauthorised access by a person such as an employee who has authorisation to access the computer system for another purpose).[1040] Increasing technological convergence means that the demarcation between communications and computer technology and between interception and hacking may be diminishing. The interception of communications could potentially be achieved by computer hacking; for example, oral and email communications relayed over the internet, or text messages relayed by internet-capable cell phones.

10.53 One distinguishing feature between the offences for interception and hacking has been the different warrant regimes that apply in each case. The interception warrant regime[1041] is more restrictive and therefore more privacy-protective than the search warrant regime[1042] (although the criteria of the interception warrant regime give it a narrower scope). However, the Search and Surveillance Powers Bill 2008 proposes that the interception and search warrant regimes be aligned. This may allow consideration to be given to whether the offences should also be more closely aligned.

10.54 One of the issues with reform of the interception offence is the impact of any such reform on law enforcement agencies. Currently, the interception of "non-private" communications is not an offence and so an interception warrant is not required. Any broadening of the range of communications subject to the interception offence would therefore require law enforcement agencies to obtain interception warrants in a broader range of circumstances, unless there was a statutory exception.

Participant monitoring

10.55 This leads to the question of what sort of other exceptions or defences should apply to the interception offence. At present, there are a number of exceptions to the offence, as outlined in chapter 9. One of the significant exceptions is participant monitoring, where one party to the communication records it without the other person's knowledge or consent (principal party monitoring), or one party to the communication consents to someone else intercepting the communication without the knowledge or consent of the other parties (authorised outsider monitoring).

1037 California Penal Code, s 632.6.

1038 California Penal Code, s 632.7.

1039 Crimes Act 1961, ss 249-252.

1040 Crimes Act 1961, s 252(2).

1041 Crimes Act 1961, Part 9A.

1042 Summary Proceedings Act 1957, s 198.

10.56 In its report on *Search and Surveillance Powers*, the Law Commission agreed with that position, and took the view that the warrant regime for law enforcement agencies should mirror it with respect to audio recording of conversations. The Search and Surveillance Powers Bill 2008 provides that no warrant is required by a law enforcement officer to make a covert audio recording of a voluntary oral communication between two or more persons with the consent of at least one of them.[1043]

10.57 Views in overseas jurisdictions diverge on this question. Some argue that the recording of one's own conversations is a permissible extension of the right to make written notes of a conversation. A contrary view is that covert recording raises different considerations to note-taking. The arguments against permitting participant monitoring are set out in the New South Wales Law Reform Commission report on surveillance,[1044] while the dissenting opinion of Justice Adams sets out the arguments in favour of allowing principal party recording as an exception to the interception offence, although his dissent does not extend to allowing authorised outsider monitoring.[1045]

10.58 Like the position in New Zealand, participant monitoring is not a criminal offence in Queensland.[1046] In Victoria,[1047] the Northern Territory of Australia[1048] and South Australia,[1049] the legality of participant monitoring is limited to principal party recording. In New South Wales, participant monitoring is permitted where reasonably necessary for the protection of a principal party's lawful interests or where the recording will not be disclosed to anyone other than the principal parties and any outsiders authorised by a principal party.[1050] In Western Australia, participant monitoring is permitted where there are reasonable grounds to believe that use of a listening device is in the public interest.[1051]

10.59 In the United States, 12 states[1052] forbid the recording of private conversations without the consent of all parties, while 38 states (plus the District of Columbia) allow one party to a record a conversation without informing the other parties.[1053] The federal wiretap law permits surreptitious recording of conversations where

1043 Search and Surveillance Powers Bill 2008, no 300-1, cl 44(1)(b).

1044 New South Wales Law Reform Commission *Surveillance: an Interim Report* (NSWLRC R98, Sydney, 2001) paras 2.99-2.107.

1045 New South Wales Law Reform Commission *Surveillance: an Interim Report* (NSWLRC R98, Sydney, 2001) Appendix A.

1046 Invasion of Privacy Act 1971 (Qld), ss 43(1), 43(2)(a) and 42(2).

1047 Surveillance Devices Act 1999 (Vic), ss 6(1) and 3(1) (definition of "party").

1048 Surveillance Devices Act 2007 (NT), ss 11(1) and 4 (definition of "party").

1049 Listening and Surveillance Devices Act 1972 (SA), ss 4 and 7(1). Participant recording is limited to the use of a listening device in the course of the person's duty, in the public interest or for the protection of the person's lawful interests: s 7(1)(b).

1050 Surveillance Devices Act 2007 (NSW), ss 7(1) and (3).

1051 Surveillance Devices Act 1998 (WA), s 26.

1052 California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington: Greg P Leslie (ed) *The First Amendment Handbook* (The Reporters Committee for Freedom of the Press, 2003) www.rcfp.org (accessed 20 October 2008). See also "Can We Tape" (2008) 32 News Media Law A1.

1053 Greg P Leslie (ed) *The First Amendment Handbook* (The Reporters Committee for Freedom of the Press, 2003) www.rcfp.org (accessed 20 October 2008).

one party consents, "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."[1054]

10.60 The Commission is interested to know whether there is agreement with the position it has taken, in other words that both kinds of participant monitoring should continue to be exceptions to the interception offence. If not, in what circumstances, and for what purposes, should participant monitoring be permissible?[1055]

10.61 Another issue is whether the authorised outsider monitoring exception should continue to be a permitted exception to the interception offence for all types of interception. There may be a case for limiting this sort of monitoring to the use of listening devices to intercept private conversations, and excluding the exception for other types of private communication such as text messages, emails and computer data, given the alternatives to interception for these types of communication. For example, a principal party can forward a message to an authorised outsider following receipt of a communication.

10.62 A further issue is whether there should be specific restrictions on the disclosure of information obtained through participant monitoring (aside from the information privacy principles in the Privacy Act 1993). Section 216C of the Crimes Act 1961 prohibits the disclosure of intercepted communications (except in certain circumstances), but this prohibition only applies to unlawful interceptions and so does not restrict the disclosure of information intercepted through participant monitoring. The position is similar in New South Wales.[1056] The Surveillance Devices Acts in Victoria,[1057] Western Australia[1058] and the Northern Territory of Australia,[1059] and the Queensland Invasion of Privacy Act 1971,[1060] however, impose controls on the disclosure of intercepted communications that includes material obtained through participant monitoring. Disclosure is only permitted in certain circumstances, such as in the public interest. One option might be to restrict disclosure of information obtained through participant monitoring only to certain groups, such as law enforcement agencies and legal counsel.

1054 Wire and Electronic Communication and Interception of Oral Communication Act 18 U.S.C. § 2510 et seq.; Greg P Leslie (ed) *The First Amendment Handbook* (The Reporters Committee for Freedom of the Press, 2003) www.rcfp.org (accessed 20 October 2008).

1055 It should be noted that, regardless of the availability or otherwise of criminal sanctions, it may, depending on circumstances sometimes be "unfair" to record one's own conversations, and thus be in breach of the Privacy Act's principle 4: see *Talbot v Air New Zealand* [1995] 2 ERNZ 356 (CA); *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 (CA) and also the case described in Privacy Commissioner "Report of the Privacy Commissioner for the year ended 30 June 1997" [1996-1999] III AJHR 11A para 3.3, as summarised by Paul Roth *Privacy Law and Practice* (loose leaf, Brookers, Wellington, 2008) PVA6.7(e).

1056 Surveillance Devices Act 2007 (NSW), s 11(1).

1057 Surveillance Devices Act 1999 (Vic), s 11.

1058 Surveillance Devices Act 1998 (WA), s 9.

1059 Surveillance Devices Act 2007 (NT), s 15.

1060 Invasion of Privacy Act 1971 (Qld), s 45.

Q41 Does the definition of "private communication" for the purposes of the interception offence require reform?

Q42 Should the participant monitoring exception to the interception offence be reformed in any respect?

Q43 Are any other reforms of the interception offence required?

Q44 Are any other reforms required in relation to communications privacy?

Tracking

10.63 At the time the tracking devices regime to regulate the use of tracking devices by law enforcement officers was being considered by the Foreign Affairs, Defence and Trade Select Committee, the Privacy Commissioner submitted that an offence provision was an essential component of the scheme if it was to fully protect privacy:[1061]

> I support the scheme proposed in this bill for the authorisation of the use of tracking devices for law enforcement purposes. However, that scheme is incomplete without the accompaniment of an offence provision. Without an offence provision the law is silent in respect of the covert use of tracking devices by citizens against other citizens, notwithstanding the effect on privacy … An offence provision would also mean that public officials, whether authorised or not, could not use tracking devices for purposes not contemplated by this scheme (such as investigating behaviour which does not constitute an offence). The offence provision would also criminalise the unauthorised placing of tracking devices on other people's vehicles, property and persons by private individuals or organisations.

The Committee disagreed that an offence provision was necessary in relation to tracking devices: "At this time, there is no evidence that the illegitimate use of tracking devices is a problem in New Zealand."[1062] However, the Committee did urge the Government to consider the recommendation of the Privacy Commissioner in the near future.

10.64 Offences have been created in various Australian states against the use of tracking devices to determine the location of a person or an object without the person's consent.[1063] There is no public interest defence that would permit the covert use of tracking devices by anyone other than law enforcement agencies

1061 Privacy Commissioner *Report to the Minister of Justice in relation to the Counter-Terrorism Bill* (7 February 2003).

1062 Foreign Affairs, Defence and Trade Committee "Counter-Terrorism Bill" (8 August 2003) 12.

1063 Surveillance Devices Act 1998 (WA), s 7(1); Surveillance Devices Act 1999 (Vic), s 8(1); Surveillance Devices Act 2007 (NT), s 13(1); Surveillance Devices Act 2007 (NSW), s 9(1).

under a tracking device warrant. In New Zealand, the Search and Surveillance Powers Bill provides that law enforcement officers must obtain a warrant to use a tracking device.[1064]

10.65 The question for consideration is whether, given developments in technology and the enactment of tracking device offences in states of Australia, it would now be desirable to enact a similar offence in New Zealand.

Q45 Should a new offence be created to target the covert use of tracking devices to determine people's locations?

Monitoring data

Spyware

10.66 Some jurisdictions have passed specific legislation dealing with aspects of computer spyware. For example, the State of California has passed the Consumer Protection Against Computer Spyware Act 2004, with the intent of protecting consumers from the use of spyware and malware that is deceptively or surreptitiously installed on their computers, including the collection of certain personally-identifiable information such as name, credit card numbers, passwords, social security numbers, addresses, payment and purchase details and Web-surfing histories.

10.67 In 2004, the Australian Government reviewed Australian laws, including the Criminal Code Act 1995 (Cth) and the Privacy Act 1988 (Cth), and their coverage of malicious spyware practices. The review found that the most serious and culpable uses of spyware (including invasion of privacy) are covered under existing legislation.[1065] A subsequent discussion paper focussed on other measures to control spyware, including best practice, technical measures to combat spyware, international co-operation and awareness-raising.[1066]

10.68 Our initial view is that the covert uses of spyware that we have considered are largely covered by the computer misuse offences, given the reasonably broad interpretation these offences have been given by the courts. The question is whether it would be useful to undertake a similar review to that done in Australia to specifically review the adequacy of these offences.[1067]

1064 Search and Surveillance Powers Bill 2008, no 300-1, cl 46(a).

1065 Australian Government, Department of Communications, Information Technology and the Arts *Outcome of the Review of the Legislative Framework on Spyware* (March 2005).

1066 Australian Government, Department of Communications, Information Technology and the Arts *Spyware Discussion Paper* (May-June 2005).

1067 Such a review could possibly be co-ordinated under the Government's *Digital Strategy 2.0* www.digitalstrategy.govt.nz (accessed 17 November 2008).

Call data

10.69 Call data (information such as phone records that includes the time and duration of a communication and the source and recipient of the communication, but excluding the content of the communication) is currently dealt with under the Telecommunications Act as a matter of civil liability.[1068] The restrictions in the Telecommunications Act apply to the attachment of equipment to a telecommunications network, but as noted in scenario 12 in chapter 9, there may be situations where call data can be monitored without attaching any equipment to a network (for example, through the use of spyware).

10.70 There is no criminal offence for the unauthorised monitoring or collection of call data. There may be a case for introducing an offence (subject to a warrant or other law enforcement exception) if call data monitoring is considered to be sufficiently intrusive to justify criminalisation. The computer misuse offences may be sufficient, although, as noted in scenario 12, these offences could be avoided where spyware is planted on a device which is then given or sold to another person and monitored by the person who installed the spyware.

10.71 Alternatively, this could be dealt with as a civil matter under a tort, or under the Privacy Act.

RFID skimming

10.72 One area that is not clear is whether the computer misuse offences would cover RFID skimming. There is a question as to whether an RFID chip would fall within the definition of "computer system" in section 248 of the Crimes Act. An RFID chip could be "stored data" for purposes of part (b) of the definition, but it is not clear whether stored data needs to be related to the items listed in part (a) (computers and communications links between them and remote terminals). If so, RFID chips may fall outside the definition of "computer system".

10.73 The State of California has recently passed a law that makes it illegal to take information from RFID tags embedded in identification documents such as driver's licences, identification cards, health insurance and benefit cards, and library cards, without an owner's knowledge and permission.[1069] There are exemptions that allow emergency medical workers to scan RFID tags to identify unresponsive people, and to allow law enforcement to scan RFID tags to solve crimes (under warrant).

10.74 The question we raise is whether an offence against RFID skimming should be considered in New Zealand.

1068 There is also a call data warrant regime for the police and customs under the Telecommunications (Residual Provisions) Act 1987 (to be repealed upon enactment of the Search and Surveillance Powers Bill 2008, cl 238).

1069 Bill Number SB 31 (introduced by Senator Joe Simitian) adding Title 1.80 to Part 4 of Division 3 of the California Civil Code; see KC Jones "California Bans RFID Skimming" (2 October 2008) *Information Week* www.informationweek.com (accessed 20 October 2008).

Q46 Are the computer misuse offences adequate to deal with privacy intrusions from computer hacking and other unauthorised access to computers and digital devices, and the use of spyware and keystroke loggers? Is a specific review of the adequacy of these offences required?

Q47 Should consideration be given to an offence for the unauthorised monitoring or collection of call data? Or should this be dealt with as a matter of civil liability?

Q48 Should consideration be given to an offence against RFID skimming in New Zealand?

REGULATORY REGIMES

10.75 We now examine the possibilities for expanding our current regulatory regimes to deal more fully with surveillance.

Privacy Act or new Surveillance Act

10.76 A key issue for consideration is whether the application of the Privacy Act principles to surveillance should be clarified, whether the privacy principles require any modification in the way they apply to surveillance, or whether a new set of surveillance principles is needed, either within the Privacy Act framework or under a new Surveillance Act framework.

Are the existing privacy principles adequate controls on surveillance?

10.77 Some of the key controls on surveillance in the Privacy Act are the "collection" principles (information privacy principles 1 to 4). There are questions, however, about how effectively these principles provide controls on surveillance. We discussed in chapter 3 the questions raised by Paul Roth about the application of the collection principles, and especially principle 3, to surveillance. While Roth's interpretation of this aspect of the Act is disputed, it could be advisable to amend the Act to make it absolutely clear that it does apply to the collection of information by the use of surveillance devices.

10.78 In relation to principle 1, there is a question as to whether the principle is overly permissive in the context of surveillance, as a broad lawful purpose may authorise an agency to collect a vast amount of personal information, in order to capture a small percentage of personal information which is relevant to the purpose. One option may be to consider whether a "minimum collection" principle is needed; that is, an agency should only collect the minimum amount of personal information necessary to achieve the intended purpose. Such a principle could assist to protect against the risk of "dragnet surveillance" and place an onus on agencies to put appropriate limitations on the collection of personal information through surveillance.

10.79 There is also a question about whether principle 4 is a sufficient control on overt surveillance. The initial act of overt surveillance is less likely than covert surveillance to be unfair or unlawful, and overt visual surveillance in public

places is less likely to intrude upon personal affairs. Nevertheless, overt surveillance may potentially impact on privacy, depending on how issues such as retention, security, use and disclosure of recorded material are handled.

10.80 There are further issues about how the other privacy principles operate with respect to surveillance. The data protection framework embodied in the privacy principles relies on people being aware of the collection of personal information so that they can exercise their rights to access and correct their personal information and bring a complaint against the collecting agency where their information has not been fairly handled in accordance with the privacy principles. The principles therefore set out presumptions that personal information will be collected directly from the person concerned (principle 2) and that he or she will be made aware of details of the collection (principle 3), although there are a range of fairly broad exceptions.

10.81 Where personal information is collected through surveillance, it could be argued that the person concerned may not have sufficient information to enforce these data protection rights, unless there is adequate notification. This may suggest that, in relation to surveillance, the presumption of notice may need to be strengthened so that there is a real opportunity for people to exercise the rights provided by the data protection framework. Strengthening of the notice principle could establish a presumption that surveillance should generally be conducted overtly and limit the circumstances in which covert surveillance may be used.

10.82 Furthermore, the information privacy principles are directed towards informational privacy. Surveillance can impact on both informational and spatial privacy, and so the existing information privacy principles may need some adjustment.

10.83 An additional point is whether the "domestic affairs" exception in section 56 of the Privacy Act is overbroad in its protection of individuals who carry out surveillance for their own personal purposes. It may be useful to retain the domestic affairs exception for certain surveillance (such as home security, the monitoring of children and dependents, and the recording of events for the family archives). However, there may be a case for ensuring that the domestic affairs exception does not permit unlawful, unfair or unreasonably intrusive surveillance of family members or others (such as neighbours or visitors).

10.84 Finally, there may be a case for a more restrictive set of principles that would apply to covert surveillance, on the grounds of the gravity of the privacy intrusion caused and the absence of notice to the person under surveillance. For example, to control the surreptitious collection of information by agencies, a purpose principle for covert surveillance might be more restrictive than principle 1 (which allows the collection of personal information that is reasonably necessary for any lawful purpose).

A new set of surveillance principles?

10.85 As an alternative to applying the privacy principles to surveillance, one option might be to create a new set of principles specifically for surveillance. A new set of surveillance principles could be included in the Privacy Act framework, or in a new Surveillance Act.

10.86 For example, the New South Wales Law Reform Commission recommended a completely new set of principles for overt surveillance (although these were not adopted).[1070] The 8 principles proposed for overt surveillance were:

- **Overt surveillance must only be undertaken for an acceptable purpose:** specifically the protection of the person, protection of property, protection of the public interest or protection of a legitimate interest. Use of surveillance by public bodies must also be in the interests of the general public.
- **Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy.**
- **Overt surveillance must be conducted in a manner which is appropriate for purpose** (intended to be developed in codes of practice)
- **Notice provisions shall identify the surveillance user**: to support the public's right to know who is watching them.
- **Surveillance users must be accountable for their surveillance devices and the consequences of their use**. This was to involve registers of surveillance devices (other than news gathering equipment) under regulations, with surveillance devices to be available for inspection by the Privacy Commissioner to monitor compliance and to investigate complaints.
- **Surveillance users must ensure that all aspects of surveillance systems are secure**. The intention of the principle was to ensure the integrity of the system and the confidentiality of the material collected.
- **Material obtained through surveillance to be used in a fair manner and only for the purpose obtained.** This was intended to ensure compliance with prohibitions such as no unauthorised viewing, listening, copying, transfer or conversion to another format, access, amendment, deletion or alteration.
- **Material obtained through surveillance to be destroyed within a specified period.**[1071] The New South Wales Law Reform Commission felt that 21 days was a reasonable period, with extensions of time under the authorisation of a judge.

The media were to be exempted from a number of these principles.

10.87 Breach of these principles would give rise to civil liability; a complaint would first be conciliated by the Privacy Commissioner and then heard by a specialist division of the Administrative Decisions Tribunal, which would have the power to order a range of remedies.

1070 New South Wales Law Reform Commission *Surveillance: An Interim Report* (NSWLRC R98, Sydney, 2001) recommendation 17, 179-193; New South Wales Law Reform Commission *Surveillance: Final Report* (NSWLRC R108, Sydney, 2005) recommendation 1, 58-71.

1071 Material obtained overtly and genuinely for media purposes to be exempt from this principle.

Jurisdiction

10.88 A further question is whether the Privacy Act jurisdiction is the appropriate level for civil complaints relating to intrusive surveillance. There are advantages for complainants in being able to access the Privacy Commissioner's complaints determination process (low cost, lower-profile forum, the philosophy of resolving complaints speedily and efficiently, and the specialist nature of the Human Rights Review Tribunal).[1072] The Human Rights Review Tribunal also has powers to grant a range of remedies including damages, and orders in the nature of injunctions that restrain continuing or repeated intrusions into privacy.[1073] The complaints determination process for privacy complaints will be further considered in Stage 4 of our Review.

Public surveillance by public entities and private entities

10.89 There is also a fundamental question about whether there should be any restrictions on who may carry out surveillance of public spaces. Should public surveillance be carried out only by public entities such as law enforcement agencies and councils? Or should private entities and members of the public also be permitted to carry out surveillance of public spaces?

10.90 A secondary question is whether there should be any limitations on the purposes for which public surveillance is conducted. There may be a case for reserving surveillance carried out by public agencies for situations where there is a clear public interest in surveillance as the method of collection, such as public safety and security and the protection of property.[1074] Restricting the purposes for which surveillance may be conducted may help to manage any risk that surveillance carried out by public authorities interferes with rights and freedoms contained in the Bill of Rights Act.

10.91 The related issue is whether there should be any controls on the surveillance of public places or privately-owned places that are open to the public by non-public entities (such as business owners). For example, in its 1998 report, the Irish Law Reform Commission proposed safeguards for visual surveillance of places frequented by the public (although these were not implemented). The main requirements for such surveillance were that notice should be provided, and that there should be limitations on the use or disclosure of information obtained through surveillance:[1075]

- Private surveillance of public places from private premises would only be permitted by premises' owners for security purposes, and provided that notice is placed on the premises in the immediate vicinity of the public place.
- Private surveillance of private places open to the public would only be permitted if notice is placed at the entrance.

1072 See New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) 35-36.

1073 Privacy Act 1993, s 85(1).

1074 See also the public interest purposes in the Privacy Act 1993, s 6, principle 2(2)(d) and principle 3(4)(c).

1075 Law Reform Commission of Ireland *Privacy: Surveillance and the Interception of Communications* (LRC 57-1998, Dublin) 156-157, 160-161. Safeguards were also proposed in relation to overt and covert surveillance by the police.

- Information obtained from permitted surveillance could only be used for the purpose for which it was obtained or to comply with a court order.
- Information obtained in breach of these controls could not be disclosed other than to law enforcement.

The Commission envisaged that there would be criminal sanctions for failure to comply. The same considerations would be relevant in relation to a regulatory regime not dependent on criminal sanctions.

Q49 Should the application of the Privacy Act to surveillance be clarified? If so, how should this be done?

Q50 Do the privacy principles need any modification in the way they apply to surveillance? If so, how should they be modified?

Q51 Is a new set of surveillance principles required, either within the Privacy Act framework or under a new Surveillance Act? If so, what should be the content of these principles, and how should they operate?

Q52 Should there be limitations on surveillance of public spaces carried out by both public and non-public agencies?

Specific regulatory options: CCTV

10.92 In addition to the surveillance framework options raised above, there are also options for controlling mass surveillance systems such as CCTV through specific regulatory mechanisms, such as specific legislation, regulations, a code of practice, guidelines or standards.

Legislation and regulations

10.93 Some countries have passed specific legislation regulating the use of CCTV systems in some contexts. The French law requires specific security purposes to be enunciated to set up a CCTV system in a public area, with various administrative approvals required. The public must be clearly informed of the presence of CCTV cameras and of the authority or person legally responsible for them. Cameras must not film the interior of or entrance to a house. Recordings may not be retained beyond one month except in the case of criminal proceedings.[1076]

1076 European Commission for Democracy through Law (Venice Commission) *Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights* (Study No. 404/2006, Strasbourg, 23 March 2007) para 71.

10.94 In 2000, a Surveillance Cameras (Privacy) Bill was introduced in the Australian Capital Territory, although the Bill lapsed on polling day for the 2001 general election. The main features of the Bill included 10 Surveillance Camera Principles and a Model Surveillance Camera Code.[1077] The Surveillance Camera Principles provided for:[1078]

- Limiting the purposes for which public surveillance cameras can be used (to deter or prevent the commission of offences, to assist in the prosecution of offences or related civil proceedings, to enforce laws imposing civil penalties and to protect public revenue).
- Surveillance only to be authorised on certain grounds (surveillance would promote a permissible purpose, no reasonable alternative, the benefit substantially outweighs any infringement of privacy and other rights).
- Surveillance not to be undertaken by unlawful or unfair means.
- A requirement for signage giving notice of surveillance.
- Reasonable measures to be taken to protect surveillance records against misuse and unauthorised use or disclosure.
- Surveillance record-keeper to take measures to assist with access to records.
- Limiting the use of surveillance records to permissible purposes (or related purposes) with the following exceptions: consent from the individual, the use is necessary to prevent or reduce a serious and imminent threat to life or health of any person, the use is expressly required or authorised by or under law.
- Disclosure of personal information in surveillance records allowed only for a permissible purpose (or related purpose), except in the following circumstances: consent has been obtained from the individual concerned, the disclosure is necessary to prevent or reduce a serious and imminent threat to life or health of any person, the disclosure is expressly required or authorised by or under law.

The Bill provided that contravention of any of the Surveillance Camera principles and contravention of the Surveillance Camera Code would be an offence, but again the above principles would also be relevant to a regulatory regime not dependent on criminal sanctions.[1079]

10.95 An alternative option to creating a specific statute for CCTV might be to include statutory requirements in the Local Government Act 2002. This would provide regulatory oversight and accountability for systems operated by local councils (but would not apply to other CCTV systems). As we noted in chapter 9, a number of local authorities have been developing CCTV strategies and policies. This could be made a requirement under the Local Government Act for any local authority installing public CCTV cameras.

10.96 To strengthen the accountability of agencies using CCTV (including footage obtained from other agencies), one option would be to consider public reporting obligations and self-certification that use of CCTV is compliant with the Privacy

1077 The Model Code dealt with matters relating to authorisation, training, and annual independent evaluations.

1078 Surveillance Cameras (Privacy) Bill 2000 (ACT), sch 1.

1079 Surveillance Cameras (Privacy) Bill 2000 (ACT), cl 6.

Act and with any guidance on the use of CCTV issued by the Privacy Commissioner.[1080] This option could be developed particularly for public agencies, or for any agency using CCTV.

10.97 In terms of the content of any such regulation, some of the issues that could be covered are indicated by the ACT Bill discussed above.[1081] A proposal put forward by a Canadian commentator is that regulation of CCTV surveillance should differentiate between collection and analysis.[1082] The idea is that the collection of images by CCTV would largely be automated, with the CCTV operator only being authorised to take manual control and engage in targeted surveillance if he or she observes something potentially criminal (or directly related to the purpose for which the CCTV system was established). Access to CCTV footage for analysis by police, or to apply particular techniques such as facial recognition software or data-matching, would require judicial authorisation, except in urgent circumstances.

CCTV guidelines

10.98 Another approach taken to CCTV by Privacy Commissioners overseas has been to issue Codes of Practice or guidelines. The UK Information Commissioner first issued a CCTV Code of Practice in 2000 and the latest version was released in 2008.[1083] The Code of Practice is aimed at businesses and organisations that routinely capture images of individuals on CCTV.

10.99 Some key suggestions in the code include:

- carrying out a privacy impact assessment prior to establishing a CCTV system;[1084]
- establishing procedures for using the system, including clearly defined specific purposes for the use of images, and the general handling of personal information;[1085]
- undertaking regular reviews of whether the use of CCTV continues to be justified;[1086]
- not using CCTV to record conversations;[1087]
- controlling disclosure of images and ensuring that disclosure is consistent with the purpose for which the system was established;[1088]

1080 The Office of the Privacy Commissioner is currently working on guidance for CCTV.

1081 See also Constitution Project Liberty and Security Committee *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties* (Constitution Project, Washington (DC), 2007), which includes model legislation for state and local governments in the United States.

1082 Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta L Rev 43, 75.

1083 Information Commissioner's Office *CCTV Code of Practice* (2008). Note that the ICO Codes of Practice have no legal status, unlike Codes of Practice issued under the New Zealand Privacy Act 1993, Part 6.

1084 Information Commissioner's Office *CCTV Code of Practice* (2008), section 4.

1085 Information Commissioner's Office *CCTV Code of Practice* (2008), section 5.

1086 Information Commissioner's Office *CCTV Code of Practice* (2008), section 5.

1087 Information Commissioner's Office *CCTV Code of Practice* (2008), section 7.

1088 Information Commissioner's Office *CCTV Code of Practice* (2008), section 8.2. This section notes that even if a system is not established to prevent and deter crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

- not keeping images for any longer than necessary;[1089]
- using clear signage to alert people to the CCTV system; and[1090]
- licensing CCTV operators if the CCTV system covers a public space.[1091]

10.100 The Privacy Commissioner of Canada has issued CCTV guidelines for both the public[1092] and private sectors.[1093] The guidelines include requirements for notification and the application of fair information practices. These guidelines do not have legal status but represent the Privacy Commissioner's interpretation of how Federal privacy legislation applies to CCTV. The Privacy Commissioner has indicated that failure to comply with the guidelines may result in her finding a violation of privacy legislation.[1094]

10.101 The New Zealand Privacy Commissioner is currently working on guidance on the use of CCTV. In addition, as we discussed in chapter 9, there is an existing Police policy document on CCTV in public places, and this could be more widely promoted.

Standards

10.102 Standards Australia has developed a set of standards for CCTV covering management and operation, including privacy issues.[1095] There are no CCTV standards in New Zealand, nor are there any joint Australian/New Zealand standards. One possible option may be to encourage Standards New Zealand to consider developing CCTV standards for New Zealand, to which the Privacy Commissioner could contribute. These standards could, in turn, be incorporated in relevant statutes, regulations or guidelines.

Specific regulatory options: RFID

10.103 The surveillance and privacy issues arising from RFID will not have significant impact until RFIDs become more common in everyday life. There is already debate about issues such as mandatory notification to consumers of the presence of RFID tags in products, mandatory or optional disabling of tags on purchase, the mandatory integration of privacy-enhancing technology in RFID applications and requiring privacy impact assessments prior to roll-out of an RFID application. There is also debate about the appropriate legal and policy framework that will be needed to address the ethical and privacy implications of RFID technology. One privacy organisation overseas has issued a set of guidelines for the

1089 Information Commissioner's Office *CCTV Code of Practice* (2008), section 8.3.

1090 Information Commissioner's Office *CCTV Code of Practice* (2008), section 9.1.

1091 Information Commissioner's Office *CCTV Code of Practice* (2008), section 9.4.

1092 Office of the Privacy Commissioner of Canada *Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (2006).

1093 Office of the Privacy Commissioner of Canada (in collaboration with the Offices of the Information and Privacy Commissioners of Alberta and British Columbia) *Guidelines for Overt Video Surveillance in the Private Sector* (2008). The Office of the Privacy Commissioner of Canada has also released a draft *Guidance on Covert Video Surveillance in the Private Sector* (October 2008) that relates to workplace surveillance.

1094 Derek Lai "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007) 45 Alta L Rev 43, 61.

1095 "Closed Circuit Television (CCTV) – Management and Operation" (AS 4806.01-2006).

commercial use of RFID technology.[1096] The European Commission is considering proposing legislation.[1097] A number of RFID consumer-protection bills have been introduced in various parts of the United States, but generally have not passed.[1098]

10.104 It would likely be premature to establish a regulatory framework for RFIDs in New Zealand at this point. It may be desirable to monitor international initiatives, and to evaluate the operation of the voluntary New Zealand RFID code of practice referred to in chapter 9, before assessing a suitable framework for New Zealand. Eventual policy decisions in this area could be informed by any new framework established for surveillance generally and for CCTV specifically.

Q53 Should CCTV be regulated under a specific CCTV statute?

Q54 If not, should CCTV be regulated in any other way such as:

- the Local Government Act;
- statutory regulations;
- a Code of Practice issued by the Privacy Commissioner;
- voluntary guidelines issued by the Privacy Commissioner; or
- standards developed by Standards New Zealand?

Q55 What are the most important issues that any regulation of CCTV should cover?

Q56 Are any specific regulatory measures needed in relation to RFID technology?

Q57 Are any other regulatory measures necessary or desirable in relation to surveillance?

1096 Electronic Privacy Information Center (EPIC) *Guidelines on Commercial Use of RFID Technology* (9 July 2004).

1097 Privacy International "Radio Frequency Identification (RFID)" (18 December 2007) www.privacyinternational.org (accessed 31 October 2008).

1098 Katherine Albrecht "RFID tag – You're it" (September 2008) *Scientific American* 76. However, California has passed a law prohibiting RFID skimming of identification documents, see para 10.73.

Chapter 11
Intrusion

11.1 In chapters 6 and 7 we discussed the tort of disclosure of private facts. The disclosure tort provides a remedy where private facts about a person are publicised in a highly offensive manner and legitimate public concern is not sufficiently strong to justify such publication. However, breaches of privacy can occur not only through disclosure of private facts, but also through interferences with people's control over access to themselves and their private affairs. We will refer to such interferences as "intrusion". The various types of surveillance discussed in the preceding chapters are examples of intrusion. In this chapter, we look at other examples of intrusion, and at whether any additional remedies may be needed either for specific forms of intrusion or for intrusion generally. In particular, we examine the possibility of introducing a tort of invasion of privacy by intrusion, which would complement the existing disclosure tort.

WHAT IS INTRUSION AND HOW CAN IT BE HARMFUL?

11.2 To intrude is to "come uninvited or unwanted; force oneself abruptly on others".[1099] The core meaning of the word, therefore, relates to unwanted access to our persons and to private spaces, or interferences with what we have called spatial privacy.[1100] The phrase "intrusion into solitude or seclusion", which is often used to summarise the United States intrusion tort, largely captures this meaning. It has been adopted in New Zealand in the BSA's privacy principles. In addition, the United States intrusion tort covers prying into a person's "private affairs or concerns", which need not involve an interference with spatial privacy and is more concerned with informational privacy. Intrusions often result in others gaining access to private facts about a person, and thus involve interferences with informational as well as spatial privacy. However, intrusion is distinct from disclosure of private facts because an intrusion may or may not reveal private facts about a person; and if it does, the person learning the private facts may or may not disclose them further. Many people would experience the intrusion itself as an invasion of privacy, regardless of whether or not it results in unwanted disclosure of private information.

1099 Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (Oxford University Press, South Melbourne, 2005) 568.

1100 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 59.

11.3 Surveillance of the kind we have discussed in the preceding chapters can be a very significant form of intrusion. Surveillance commonly involves gaining unwanted access to a person and prying into a person's private affairs. By using devices that enhance ordinary human senses, it is possible to gain access to a person at a distance, without the person's knowledge or consent.

11.4 In addition to surveillance, there are a range of other forms of intrusion, including:

- physical intrusions into spaces where a person or persons could reasonably expect to be left alone;
- searches of private spaces (such as rooms, vehicles or lockers);
- access to personal objects that a person could reasonably expect not to be opened or interfered with (such as bags, diaries, private mail, cellphones or computers);
- unauthorised access to private records about a person (such as a person's medical records);
- sustained watching of others without the use of devices ("peeping Tom" activity);
- unwanted communications (such as repeated, unsolicited phone calls);
- strip searches, either using the unaided sense of vision or using machines that can "see" through clothes and create detailed images of people's bodies;[1101] and
- unauthorised collection and testing of bodily samples.

11.5 Intrusions into solitude and seclusion interfere with the interests of individuals and small groups in having time apart from others for activities such as reflection, rest, recuperation, relaxation, and private conversation. According to Daniel Solove, intrusion "disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy."[1102] As Solove further points out, there is a social as well as an individual interest in protecting solitude and seclusion:[1103]

> Solitude enables people to rest from the pressures of living in public and performing public roles. Too much envelopment in society can be destructive to social relationships … Without refuge from others, relationships can become more bitter and tense. Moreover, a space apart from others has enabled people to develop artistic, political, and religious ideas that have had lasting influence and value when later introduced into the public sphere.

1101 "Camera 'Looks' Through Clothing" (10 March 2008) http://news.bbc.co.uk (accessed 15 September 2008); "Privacy 'Infringed' by Scanners that See Sex Organs" (11 June 2008) www.news.com.au (accessed 13 June 2008); "Passengers Feeling Exposed by Airport Device" (24 June 2008) www.ctv.ca (accessed 27 June 2008).

1102 Daniel Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477, 553.

1103 Daniel Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477, 555.

Intrusions into solitude or seclusion, unauthorised access to personal items or to a person's body, and prying into personal affairs, can also cause feelings of embarrassment, shame, humiliation, loss of autonomy, betrayal and violation. These harms are distinct from the further harms that may be caused if information obtained through intrusion is further disclosed or misused.

SOME SCENARIOS AND THE CURRENT LAW

11.6 We have already examined a number of scenarios relating to surveillance. We now consider some more scenarios involving other forms of intrusion, and relate them to current legal protections in order to identify gaps in the law. We are concerned here only with how the law protects against the intrusion itself. There may, in addition, be legal protections against disclosure of any private information learned as a result of the intrusion. For example, the Privacy Act's use and disclosure principles will apply in many cases, and a complaint can be made to the Broadcasting Standards Authority about the broadcasting of private facts.

11.7 It is also important to mention that the Privacy Act 1993 regulates the collection of personal information.[1104] Information privacy principle 4 provides that:

> Personal information shall not be collected by an agency –
>
> (a) by unlawful means; or
>
> (b) by means that, in the circumstances of the case,–
>
> (i) are unfair; or
>
> (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

11.8 Information privacy principle 4 clearly provides protection against unfair and intrusive information-gathering. It can be the basis for complaints to the Privacy Commissioner and, if the complaint proceeds to the Human Rights Review Tribunal, damages can be awarded. However, the Privacy Act's complaints provisions are limited in some respects:

- The Act's complaints provisions are focused on information, so cannot deal directly with intrusions on spatial privacy.
- As we discussed in chapter 3 and the chapters on surveillance, there is a question about whether the collection principles in the Act apply to electronic surveillance, due to the Act's definition of "collect" to exclude "receipt of unsolicited information".
- It is not clear how principle 4 applies to unsuccessful attempts to collect information. The Human Rights Review Tribunal has considered this question, but has not ruled definitively on it.[1105]
- The Act does not create legal rights that are enforceable in the courts.[1106]
- The Act does not apply to the news media in their newsgathering activities.[1107]

1104 Privacy Act 1993, s 6, information privacy principles 1-4.

1105 *Stevenson v Hastings District Council* (14 March 2006) Human Rights Review Tribunal 07/06, paras 64-72; *Lehmann v CanWest Radioworks Limited* (21 September 2006) Human Rights Review Tribunal 35/06, paras 67-68.

1106 Privacy Act 1993, s 11(2). As we noted in chapter 2, there is a limited right of direct access to the courts in s 11(1).

1107 Privacy Act 1993, s 2 (definitions of "agency" and "news activity").

Despite these limitations, it should be borne in mind that a complaint to the Privacy Commissioner could be made in a number of the scenarios set out below.

Scenario 1 – physical intrusion

11.9 ***A** is a well-known actor who is recovering from a serious head injury in a private hospital room. Ignoring clear notices restricting access to the room, newspaper journalists enter **A**'s room, take photographs of him and conduct an interview while he is in a confused state. The photographs and a story based on the interview are subsequently published in the newspaper.*[1108]

11.10 **A** would have few, if any, legal remedies for the intrusion under current law. The hospital might be able to maintain an action for trespass against the journalists, but it is unlikely that **A** could do so with respect to the intrusion into his room.[1109] The Harassment Act 1997 would only apply if the same journalists committed another "specified act" directed at **A** within a 12-month period. The intimate covert filming provisions of the Crimes Act 1961 would only apply if **A** was photographed naked or near-naked, or on the toilet. The Code of Health and Disability Services Consumers' Rights includes the right of consumers to have their privacy respected (Right 1(2)), but this is not enforceable against third parties, so **A** would have to complain that the hospital failed adequately to protect his privacy. **A** could bring an action for intentional infliction of harm, though it is questionable whether it would have any chance of success.

Scenario 2 – unauthorised access to personal objects

11.11 ***B** and **C** work in the same organisation. While **B** is in a meeting, **C** enters **B**'s office, rifles through **B**'s handbag, and looks at text messages and digital photographs on **B**'s personal cellphone. **C** does not remove anything from the handbag, nor does she use or interfere with the cellphone apart from viewing the messages and photographs.*

11.12 **C**'s actions involve unauthorised access to **B**'s personal items and prying into her personal affairs. If **C** had opened **B**'s personal mail (which is akin to reading her cellphone text messages), **C** would have committed an offence. Likewise, it would be a criminal offence for **C** to intercept **B**'s text messages in the course of transmission, but the interception offence does not cover reading stored messages by physically accessing **B**'s cellphone. The unauthorised accessing of someone else's cellphone may be in breach of section 252 of the Crimes Act 1961,

1108 This scenario is based on the facts of *Kaye v Robertson* [1991] FSR 62. For other cases involving intrusions in hospitals see *Barber v Time Inc* (1942) 149 SW 2d 291 (Mo); *Noble v Sears, Roebuck and Co* (1973) 33 Cal App 3d 654; and a case (settled before going to trial) discussed in Nick Davies *Flat Earth News: An Award-Winning Reporter Exposes Falsehood, Distortion and Propaganda in the Global Media* (Chatto & Windus, London, 2008) 389. Another possible example of physical intrusions in circumstances in which people could reasonably expect to be left alone could be intrusions at funerals by the media, protesters, or others whose presence is unwelcome. Many American states have laws restricting protests near cemeteries or funerals, and these laws are often justified on the grounds that they protect the privacy of mourners: Christina E Wells "Privacy and Funeral Protests" (forthcoming) NCL Rev, currently available in draft at http://ssrn.com.

1109 John Smillie "Trespassing on Land" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 360, 368. However, in *Hosking v Runting* [2005] 1 NZLR 1 (CA), para 269, Anderson J suggested that in the circumstances of *Kaye v Robertson* "there could have been no question of an implied licence to enter the hospital room and photograph the injured patient, so that the people who took the photograph must have been trespassers".

which deals with accessing of computer systems without authorisation. The definition of "computer system" in the Act does not define "computer", and it could be argued that modern cellphones are a type of computer.[1110] If cellphones are covered by the computer crimes sections of the Crimes Act, then the very broad terms of section 252 mean that it would probably be an offence to access a cellphone without authorisation, although it might be at the low end of the scale of an offence designed primarily to deal with computer hacking.[1111]

11.13 It is also arguable that **C**'s actions constitute trespass to goods, but the question of whether touching goods without authority is a trespass if no damage results is currently unsettled in New Zealand law.[1112] Interference with property in a person's possession is a "specified act" under the Harassment Act 1997, so if **C** committed another specified act directed at **B** within a 12-month period, **B** could seek a restraining order against her.

11.14 Finally, **B** could complain about **C**'s actions to the employer, who would probably have good grounds for taking disciplinary action against **C** for misconduct.

Scenario 3 – watching without using devices

11.15 ***D**'s bedroom window is close to the street. When she is in her bedroom during the day, **E** stands outside the window looking in until she notices him and he runs away.*

11.16 If **E** had peered in **D**'s window at night, he could be charged with peeping or peering into a dwellinghouse under section 30(1) of the Summary Offences Act 1981. If **E** were to peer into her window at least once more or commit another "specified act" within a 12-month period, **D** could seek a restraining order against him under the Harassment Act 1997. If **E** ventured onto **D**'s property at all, she could bring an action for trespass, and if he refused to leave the property after being asked to do so he could be charged with a criminal offence under the Trespass Act 1980. If **E** is standing on a public street, he could perhaps be charged with offensive behaviour in a public place under section 4(1) of the Summary Offences Act.

11.17 *Some months later, **D** finds holes cut in the bathroom floor, and reports this to the Police. The Police set an alarm and a dye trap under the house, and catch **E**, who has been crawling under the house to look through the holes at **D** when she is in the bathroom.*[1113]

11.18 Again, unless there is evidence that **E** had been watching **D** at night, he could not be charged with peeping and peering. He could be charged under the Summary Offences Act with wilful damage to property or being on a property

1110 David Harvey *Internet.law.nz: Selected Issues* (LexisNexis, Wellington, 2005) 210. The definition of "computer system" is in section 248, which states that the definitions in that section apply to sections 249 and 250. It seems likely that the definitions in section 248 should also apply to sections 251 and 252.

1111 Section 252 of the Crimes Act can apply to simply reading information on a computer screen without authorisation. In *R v Boyack* (6 June 2008) HC AK CRI 2007-044-002515, the offender had turned a computer monitor in a Police station towards him and used the mouse to access the Police intranet. Because of password restrictions, he was unable to get further into the system. Woodhouse J stated that this action was technically covered by section 252 of the Crimes Act, but was at the very bottom of the scale.

1112 Cynthia Hawes "Interference with Goods" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 461, 465.

1113 This part of the scenario is based on an incident reported in Theresa Garner "The Peeping Tom, the Judge and I ..." (15 January 2000) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 22 December 2008).

without lawful excuse. Since **E** has now committed two specified acts within a 12-month period, **D** could seek a restraining order against him under the Harassment Act. **E** could possibly also be charged with criminal harassment if it could be argued that he knew that his activities could cause **D** to reasonably fear for her safety. In addition, **D** could bring an action for trespass against **E**.

Other scenarios

11.19 We list below some further intrusion scenarios. For reasons of space, we do not discuss how they are covered by the current law, but we invite submitters to consider whether any additional criminal offences or civil remedies are needed for scenarios such as these.

- ***Scenario 4.*** ***F*** *is a candidate for political office. Using saliva from* ***F****'s drinking glass (left behind after a public meeting, so no issue of trespass arises),* ***G*** *obtains an analysis of* ***F****'s DNA without* ***F****'s consent.* ***G*** *discloses the fact that* ***F*** *has a particular genetic condition to a newspaper, which publishes this fact.*[1114]
- ***Scenario 5.*** ***H*** *is an academic known for his controversial views on moral issues.* ***I****, the writer of a popular blog who disagrees with* ***H****'s moral stance, posts* ***H****'s unlisted telephone number in his blog and urges readers to ring* ***H*** *to express their disagreement with* ***H****'s views. As a result,* ***H*** *receives a large number of abusive phone calls.*[1115]
- ***Scenario 6.*** ***J*** *is an employee of a district health board who has access to electronic patient medical records. Out of curiosity,* ***J*** *opens and reads the medical records of* ***K****, a television celebrity.*[1116]
- ***Scenario 7.*** ***L*** *is a newspaper reporter looking for evidence that* ***M****, a prominent businesswoman, has been engaging in tax fraud.* ***L*** *secretly goes through rubbish bags taken from outside* ***M****'s house, and rubbish bins outside the offices of her lawyer and her accountant, looking for evidence of fraud.*[1117]

1114 Based on a scenario in Human Genetics Commission *Inside Information: Balancing Interests in the Use of Personal Genetic Data* (London, 2002) 60. See also Australian Law Reform Commission and National Health & Medical Research Council – Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) 360 for alleged cases of attempts to obtain DNA samples for genetic testing without consent. The Human Tissue Act 2008, s 23, creates an offence of collecting human tissue for analysis, or carrying out analysis, without consent. However, Katie Elkin argues that, due to the definition of "human tissue", the Act does not apply to discarded tissue (such as saliva on a drinking glass): Katie Elkin "The New Regulation of Non-Consensual Genetic Analysis in New Zealand" (2008) 16 JLM 246. Possible offences for non-consensual genetic testing are under discussion in Australia: Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General *Discussion Paper: Non-Consensual Genetic Testing* (November 2008). There is also the question of what civil remedies should be available.

1115 For a somewhat similar scenario involving a radio station that was the subject of a complaint to the Broadcasting Standards Authority see *Spring v The Radio Network* (21 April 2008) Broadcasting Standards Authority 2007-108. Note that the Harassment Act 1997 could apply to this situation. Section 16(2) of the Act provides that, for the purposes of the Court's power to make a restraining order under the Act, a respondent who encourages another person to do a specified act to the complainant is regarded as having done that specified act personally.

1116 See Martin Johnston "Worker Sacked for Reading Celebrities' Health Records" (20 November 2007) *New Zealand Herald* www.nzherald.co.nz (accessed 20 November 2007); "Staff Pry into Files of Celebrity Patients" (21 November 2007) www.stuff.co.nz (accessed 21 November 2007). The Privacy Commissioner has recommended changes to the Privacy Act to deal with this issue of "employee browsing": Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review: Report of the Privacy Commissioner on the First Periodic Review of the Operation of the Privacy Act* (Office of the Privacy Commissioner, Auckland, 1998) 53-55, 73-74, recs 16 and 23.

1117 On the use by newspapers of material obtained from rubbish bins, see Nick Davies *Flat Earth News: An Award-Winning Reporter Exposes Falsehood, Distortion and Propaganda in the Global Media* (Chatto & Windus, London, 2008) 279-282.

Conclusion

11.20 The above scenarios illustrate some gaps and uncertainties in the law with regard to intrusions that do not involve the use of devices. Such gaps could be filled by specific criminal or civil provisions, or by a general intrusion tort. Alternatively, it may be considered that the gaps are not sufficiently serious, or involve matters that arise too infrequently, to warrant new laws.

SPECIFIC CRIMINAL OFFENCES AND CIVIL REMEDIES

11.21 We discussed in chapters 9 and 10 the issues surrounding the civil and criminal law relating to surveillance, and options for reform. Here we raise the question of whether reform is needed to deal with intrusions that do not involve the use of devices. Two existing statutory provisions dealing with such intrusions are the Harassment Act 1997 and section 30(1) of the Summary Offences Act 1981.

The Harassment Act 1997

11.22 We have considered in chapter 10 whether the Harassment Act should deal more explicitly with the use of surveillance for the purposes of harassment. We raised there the question of how the requirement in the Act for specified acts to occur on two or more occasions within a 12-month period should apply to continuous, ongoing surveillance. That issue aside, however, it is clearly appropriate that the Act should continue to apply only where there is a pattern of behaviour. The purpose of the Act is to deal with behaviour that could appear relatively minor when taken in isolation, but that appears more serious when viewed as part of a pattern. To make it applicable to single incidents would, therefore, fundamentally alter its nature. More serious acts of intimidation may be offences under the Summary Offences Act 1981 even if they occur on only a single occasion.[1118]

11.23 Another question concerning the Harassment Act is whether it should provide for damages, as the equivalent Act in the United Kingdom does.[1119] At present a person seeking damages for harassment could try suing under a number of torts discussed in chapter 2, including nuisance and breach of a statutory duty imposed by the Harassment Act. It also remains an open question whether or not there is a tort of harassment in the common law.[1120] There may be a case for providing expressly for damages in the Harassment Act, so that victims can be compensated for the distress caused by harassment, including distress arising from loss of privacy.

Voyeurism, including the "peeping and peering" offence

11.24 With regard to the "peeping and peering" offence in the Summary Offences Act 1981, the key questions for possible reform are whether the parameters of the offence are appropriate, and whether the penalties are adequate. There is no obvious reason for restricting the offence to peeping and peering at night (which is defined in terms of the period between sunset and sunrise). Presumably it was considered that such behaviour seemed more threatening at night, that a peeping Tom was more likely

1118 Summary Offences Act 1981, s 21.

1119 Protection from Harassment Act 1997, ss 3(2), 8(5)(a), 8(6). Section 3 applies to England and Wales and section 8 to Scotland.

1120 John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, South Melbourne, 2005) 280-281; Stephen Todd "Trespass to the Person" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 80, 112-114.

to find a woman in a state of undress after dark, and that a person was less likely to have a legitimate reason for looking into someone else's house at night. There is no such restriction in the equivalent provision in New South Wales.[1121] Another question is whether the term "dwellinghouse" is sufficiently broad to encompass a variety of buildings in which a person could reside and have a reasonable expectation of privacy. If the parameters of the offence were to be widened in some respects, particularly by making it applicable during the day, it would probably be necessary to narrow it in other respects to ensure that only offensive behaviour is targeted. One possibility, discussed below, would be to replace the current peeping and peering offence with a new voyeurism offence.

11.25 In relation to penalties, a maximum fine of $500 could be viewed as insufficient for what can be a significant invasion of privacy. The Government Administration Committee, in its report on the Crimes (Intimate Covert Filming) Amendment Bill, noted with concern that the penalty for the peeping and peering offence had not been updated since the inception of the offence in 1982.[1122] Peeping and peering commonly has a voyeuristic sexual element which, as the Law Commission noted in its study paper on intimate covert filming, has been correlated with more serious sexual offending.[1123] The equivalent New South Wales offence makes provision for imprisonment as well as fines, as did section 52A of the Police Offences Act 1927, which section 30(1) of the Summary Offences Act 1981 replaced. However, to the extent that peeping Tom activity is sexually motivated and symptomatic of a psychological disorder, the effectiveness of short prison terms may be questionable, and offenders may be in need of a treatment programme.[1124] Any change to the penalties for the offence would also need to be considered in relation to the penalties for other comparable offences.

11.26 The law currently provides only imperfect protection against another type of peeping Tom activity that does not involve the use of recording devices. This is where a person covertly observes others by drilling holes in a wall, floor or ceiling; by installing one-way mirrors; or by other means not involving recording devices. Such methods of covert observation are sometimes used by peeping Toms in places where people expect privacy, such as bathrooms, toilets, changing rooms and bedrooms. At present, depending on the particular circumstances of the offending, a peeping Tom engaging in such activity could be charged with a number of offences under the Summary Offences Act, including offensive behaviour in a public place, wilful damage to property, or being on a property without lawful excuse.[1125] These offences, however, do not directly address the invasion of privacy involved, and there may be some instances in which there is no offence with which a peeping Tom can be charged. The peeping and peering offence under the Summary Offences Act would only apply if the activity occurred at night and involved looking into a dwellinghouse. The intimate covert filming provisions of the Crimes Act 1961 deal with the covert use of visual recording devices in places where people have a reasonable expectation of

1121 Crimes Act 1900 (NSW), s 547C, refers to a person who "is in, on or near a building without reasonable cause with intent to peep or pry upon another person".

1122 Government Administration Committee "Crimes (Intimate Covert Filming) Amendment Bill" (1 August 2005) 3.

1123 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) 11-12.

1124 Alisdair A Gillespie "'Up-Skirts' and 'Down-Blouses': Voyeurism and the Law" [2008] Crim LR 370, 375.

1125 Summary Offences Act 1981, ss 4(1)(a), 11, 29.

privacy, if their naked bodies or intimate activities are exposed.[1126] However, there is no offence of covertly observing others in such circumstances without recording. This contrasts with other jurisdictions which have criminalised voyeuristic observation as well as recording.[1127]

11.27 One possibility for dealing with the gaps identified in the previous paragraph and in our discussion of the existing peeping and peering offence would be to create a new offence of voyeurism. Further thought would need to be given, however, to the parameters of such an offence. Consideration would also need to be given to whether voyeurism by means of visual recording devices, currently covered by the intimate covert filming provisions of the Crimes Act, should continue to be treated separately from voyeurism undertaken without the use of a recording device.

Other gaps

11.28 With regard to civil remedies, we discuss below whether there should be a tort of invasion of privacy by intrusion. We set out in chapter 2 some existing civil remedies for intrusion, including trespass and nuisance. We also discussed the tort of breach of statutory duty. One option for reform is that Parliament could make express provision in certain statutes protecting against intrusion for a right of civil action for breach of the statute.

11.29 There may be other gaps in the existing civil and criminal law relating to physical intrusions into privacy or prying into personal affairs (as opposed to disclosing personal information obtained through such prying). The Commission invites submitters to identify any such gaps.

Q58 Should the Harassment Act 1997 provide for the award of damages?

Q59 Are any reforms to the law needed to deal with voyeurism not involving the use of recording devices, including reform of the "peeping and peering" offence in the Summary Offences Act 1981?

Q60 Are any new criminal offences, or changes to existing offences, needed to deal with specific types of intrusion other than surveillance?

Q61 Are any new civil remedies (apart from a possible intrusion tort) needed to deal with intrusion?

Q62 Should an express right to sue for breach of statutory duty be created in relation to any statutory provisions relating to intrusion?

1126 Crimes Act 1961, ss 216G-216N.

1127 Sexual Offences Act 2003 (UK), s 67; Criminal Code Act 1899 (Qld), s 227A; Criminal Code RSC 1985 c C-46, s 162.

AN INTRUSION TORT?

11.30 As we discussed in chapter 2, the law already protects against intrusion by means of various criminal offences and civil remedies. We have considered above ways in which the law might fill specific gaps in the existing framework of legal protections, particularly in relation to surveillance. It remains to consider whether there should be a general tort of invasion of privacy by intrusion into a person's solitude, seclusion or personal affairs. In this section we discuss whether there should be an intrusion tort, how it might be introduced, what form it might take, and various specific issues that would need to be considered if there were to be such a tort. We emphasise that this would be a general tort which would cover surveillance of the kinds discussed in the preceding chapters, as well as other intrusions such as those in the scenarios set out earlier in this chapter.

11.31 It is currently an open question whether such a tort is available in New Zealand common law. In *Hosking*, Gault P and Blanchard J emphasised that their judgment was concerned only with publication of private facts, and that they did not need to decide in that case whether a tortious remedy should be available for intrusion. They noted that in many cases this aspect of privacy would be protected by the torts of trespass or nuisance, or by the Harassment Act, but that trespass might be of limited value in protecting against covert intrusions such as long-lens photography, audio surveillance and video surveillance.[1128]

Should there be an intrusion tort?

11.32 In chapter 7 we considered the arguments for and against the disclosure tort. Many of the same arguments apply to the intrusion tort. Here we consider some additional arguments that relate specifically to the intrusion tort.

Arguments against a tort

11.33 Arguments against an intrusion tort include the following:

- The law already provides many protections against intrusion. To the extent that there are gaps in the existing law (particularly in relation to surveillance) these could be plugged with specific criminal offences or civil remedies, rather than a new general cause of action.
- There would be considerable overlap in practice between an intrusion tort and the disclosure tort, as well as between an intrusion tort and the Privacy Act. It seems likely that, in most cases, the intrusion will be for the purposes of obtaining and publicising private information about a person. Therefore, while intrusion is conceptually distinct from disclosure, it may be artificial in practice to separate them. The number of cases in which there is a serious intrusion without subsequent publicity given to private facts obtained through the intrusion is likely to be small.
- The boundaries of the tort (discussed further below) are as yet unknown. It might be difficult to frame it in such a way as to exclude the kinds of intrusions into private space and private affairs that are an inevitable part of living together with other people (for example, it would not be reasonable to expect legal protection against other passengers listening in to a person's conversation on a bus).

1128 *Hosking v Runting* [2005] 1 NZLR 1 (CA), para 118.

- An intrusion tort could act as a constraint on the legitimate exposure of wrongdoing, or other forms of investigation in the public interest, by the media and others. Sometimes intrusive measures may be needed to uncover matters of public concern that particular individuals have been trying to hide. There would need to be a "public concern" defence to the tort, but we have already noted in chapter 6 the uncertainty inherent in this formulation.

Arguments for a tort

11.34 These are some arguments in favour of an intrusion tort:

- The tort would complement existing legal protections. In particular, it would:
  (a) protect spatial privacy, whereas the disclosure tort and the Privacy Act only protect informational privacy;
  (b) protect against prying into a person's private affairs, whereas the disclosure tort only protects against publicity given to private matters; and
  (c) protect against intrusions by private parties, whereas the protection against unreasonable search and seizure in section 21 of the New Zealand Bill of Rights Act 1990 only applies to intrusions by the state.
- Existing legal protections against intrusion are not comprehensive. An intrusion tort would provide a comprehensive civil remedy for intrusion, including surveillance, that would be flexible enough to deal with issues and facts that have not been anticipated.
- At its worst, intrusion into people's seclusion and private affairs can be a very serious interference with their dignity and autonomy. We have discussed the harms of surveillance in chapter 8, and the harms of other forms of intrusion at paragraph 11.5 above.
- There is existing jurisprudence in this area, from overseas as well as from New Zealand, that can be built on. The Broadcasting Standards Authority has had an intrusion principle for more than 15 years. The BSA has applied its intrusion principle to a significant number of complaints, including some that have been appealed to the High Court, and has regularly considered the balance between privacy and the public interest.[1129] The jurisprudence relating to section 21 of the Bill of Rights Act is also likely to be helpful, particularly in relation to the impact of surveillance devices on privacy.

Q63 Should there be an intrusion tort?

If there is to be a tort, should it be common law or statutory?

11.35 Even if it is considered that an intrusion tort would be desirable, one option would be to wait and see if the courts will recognise such a tort in New Zealand common law. This would mean waiting for a suitable case to test the existence of the tort. We considered in chapter 7 the arguments for the common law and for statute in relation to the disclosure tort. The same arguments apply to the

1129 Steven Price *Media Minefield: A Journalists' Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 114-121. A High Court case considering the BSA principles on both intrusion and the public interest is *CanWest TVWorks Ltd v XY* [2008] 1 NZAR 1.

intrusion tort, but with the significant difference that the intrusion tort has not yet been found to exist in common law. Statute may, therefore, be the only way to bring the intrusion tort into existence.

Q64 Should the development of an intrusion tort be left to the common law, or should it be introduced by statute?

If there is to be a statute, what should it contain?

11.36 Without prejudging whether there should be an intrusion tort at all, and whether it should be common law or statutory, we now consider what the content of the tort might be *if* it were to be introduced by statute.

The elements of the tort

11.37 There are a number of ways in which the elements of the intrusion tort could be framed. One option would be to adopt the formulation of the United States tort:[1130]

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his [or her] private affairs or concerns, is subject to liability to the other for invasion of his [or her] privacy, if the intrusion would be highly offensive to a reasonable person.

This clearly contemplates either an intrusion into a space where a person is enjoying solitude or seclusion, or an intrusion into a person's private affairs. The Law Reform Commission of Hong Kong recommended a similar form of the intrusion tort, with some small variations, including making explicit that the plaintiff must show that he or she had a reasonable expectation of privacy in the circumstances of the case.[1131]

11.38 A New Zealand variation of the United States tort can be found in the Privacy Principles of the Broadcasting Standards Authority (BSA). Principle 3 refers to "intentionally interfering, in the nature of prying, with [an] individual's interest in solitude or seclusion. The intrusion must be highly offensive to an objective reasonable person." Because the BSA's remit is to deal with broadcast material, the BSA principle also requires that there has been public disclosure of material obtained by an interference with solitude or seclusion, but the focus is on the offensiveness of the intrusion rather than the disclosure. The BSA principle does not refer to private affairs or concerns. However, the BSA has stated that the word "prying" means "inquiring impertinently into the affairs of another person" or "interfering with something that a person is entitled to keep private".[1132] The BSA principle also provides that an individual's interest in solitude or seclusion does not normally prohibit the recording of a person in a public place; however, this public place exception does not apply when a person is particularly vulnerable, and when the disclosure would be highly offensive to an objective reasonable person.

1130 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652B.

1131 Law Reform Commission of Hong Kong *Civil Liability for Invasion of Privacy: Report* (2004) 139.

1132 *Macdonald v The Radio Network* (6 May 2004) Broadcasting Standards Authority 2004-047, para 16; *Balfour v TVNZ* (21 March 2006) Broadcasting Standards Authority 2005-129, para 39.

11.39 Some commentators have preferred not to use the words "solitude and seclusion", in order to widen the scope for recognition of privacy intrusions in public and semi-public places. They consider that "solitude and seclusion" tend to suggest that privacy can only be invaded in private places or places not generally open to public view. Andrew Jay McClurg proposes the following reformulation of the intrusion tort in the United States:[1133]

> One who intentionally intrudes, physically or otherwise, upon the private affairs or concerns of another, whether in a private physical area or one open to public inspection, is subject to liability to the other for invasion of her [or his] privacy, if the intrusion would be highly offensive to a reasonable person.

McClurg proposes that this paragraph would be followed by a set of factors to be taken into account in considering whether an intrusive act would be highly offensive. Similarly, Des Butler argues that the intrusion tort should apply wherever a person has a reasonable expectation of privacy, rather than being restricted to private places. He suggests that the elements of the intrusion tort should be:[1134]

(a) an intentional intrusion (whether physical or otherwise) upon the situation of another (whether as to the person or his or her personal affairs) where there is a reasonable expectation of privacy; and

(b) the intrusion would be "highly offensive to a reasonable person of ordinary sensibilities".

11.40 The formulations of the tort discussed so far include both intrusions on the person of the plaintiff (whether physical or otherwise) and intrusions into the plaintiff's personal affairs. That is, there could be an interference with spatial privacy, or informational privacy, or both. The inclusion of prying into personal affairs brings the tort squarely into the realm of informational privacy and is, as Des Butler points out, a point of interface between the intrusion and disclosure torts: "In the first instance, there may be an intrusion in the course of the gathering of information, followed by a public disclosure of those private facts."[1135]

11.41 Alternatively, the tort could be more narrowly focused on intrusions into personal or private space, including intrusions by means of devices, but excluding the category of intrusions into a person's private affairs or concerns. This would make the tort line up more clearly with the distinction between informational and spatial privacy. For example, Rachael Mulheron proposes the following elements for the intrusion tort:[1136]

(1) An *invasion* is made into the claimant's "personal space" …

(2) The invasion must be in respect of a *personal*, as opposed to a public, *space* …

(3) The intrusion must *not* be of a *trivial* kind, and must be one that would be *highly offensive* to the ordinary person …

1133 Andrew Jay McClurg "Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places" (1995) 73 NCL Rev 989, 1058.

1134 Des Butler "A Tort of Invasion of Privacy in Australia?" (2005) 29 Melb U LR 339, 373.

1135 Des Butler "A Tort of Invasion of Privacy in Australia?" (2005) 29 Melb U LR 339, 371.

1136 Rachael Mulheron "A Potential Framework for Privacy? A Reply to *Hello!*" (2006) 69 MLR 679, 702-703. Emphasis in the original.

11.42 Finally, a statute could give specific examples of the types of invasions of privacy that are covered by the tort. For example, the statutory torts of the Canadian provinces of Saskatchewan, Manitoba and Newfoundland give examples of invasions of privacy that include various types of surveillance, interception of communications, and use of personal documents without consent.[1137] Such examples can be combined with a more general statement of the elements of the tort.

11.43 In addition, a number of the questions raised in chapter 7 with regard to the "reasonable expectation of privacy" and "highly offensive" elements of the disclosure tort are also relevant (with appropriate modifications) to the intrusion tort. If the "highly offensive" threshold continues to apply to the disclosure tort, it would undoubtedly also apply to the intrusion tort. All of the examples of formulations of the intrusion tort discussed above include the "highly offensive" test. As with the disclosure tort, one option would be to list considerations to be taken into account when assessing whether a reasonable expectation of privacy exists, or whether an intrusion is highly offensive. These considerations could differ in some respects from those for the disclosure tort.

11.44 One important question is whether there can be a reasonable expectation of privacy in a public place and, if so, in what conditions. The *Restatement of the Law of Torts* says that the United States tort does not generally recognise liability for intrusions in public places, although there are some exceptions with regard to the involuntary exposure of matters "that are not exhibited to the public's gaze", such as the plaintiff's "underwear or lack of it".[1138] The narrowness of the public places rule set out in the *Restatement* has been criticised by some commentators,[1139] and in fact it appears that the United States courts have been moving away from the mechanical application of such a rule towards a more context-specific approach.[1140] As noted above, the BSA's Privacy Principle based on the United States intrusion tort recognises that there can be an intrusion in a public place where the person concerned is "particularly vulnerable".

11.45 William Prosser explained the rule that the intrusion tort does not generally apply in public places by stating that a person has "no right to be alone" in a public place. Even if a record is created by taking a photograph of a person in public (or by using some other kind of device to record the person), this is not essentially different "from a full written description, of a public sight which any one present would be free to see".[1141] This view has been criticised for taking an "all or nothing" view of privacy, rather than seeing it as a matter of degree shaped by a number of context-specific considerations. While those who argue

1137 Privacy Act RSS 1978 c P-24 (Saskatchewan); Privacy Act CCSM 1987 c P125 (Manitoba); Privacy Act RSNL 1990 c P-22 (Newfoundland).

1138 American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652B, comment c.

1139 Andrew Jay McClurg "Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places" (1995) 73 NCL Rev 989; Elizabeth Paton-Simpson "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 U Toronto LJ 305.

1140 See the categories of exceptions to the public places rule identified by Elizabeth Paton-Simpson "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 U Toronto LJ 305, 324, 331, 334, 338; June Mary Z Makdisi "Genetic Privacy: New Intrusion a New Tort?" (2001) 34 Creighton L Rev 965, 1000-1020.

1141 William L Prosser "Privacy" (1960) 48 Cal L Rev 383, 391-392.

that there can be privacy intrusions in public places do not deny that location is a relevant factor in assessing expectations of privacy, they contend that it should not be determinative. Elizabeth Paton-Simpson writes that:[1142]

> Most people spend a great deal of their everyday lives in public places without imagining that they are being observed any more than casually and by a limited number of people. A number of factors provide varying degrees of privacy in public places. These factors include varying degrees of exposure or seclusion in different places and at different times, anonymity and the limitation of attention paid, various social rules, the dispersion of information over space and time, and the ephemeral nature of our use of public space. A rogue factor that not only disrupts normal expectations of public privacy but also undermines the distinction between public and private places is the use of privacy-invasive technologies.

As with the disclosure tort, there may be merit in spelling out the circumstances in which privacy may be intruded on in an actionable manner in a public place.

Q65 If an intrusion tort is to be introduced by statute, what should be its elements? Specifically:

- Should it refer to intrusions on "solitude and seclusion", and would this necessarily suggest that it applies only in private places?
- Should it include intrusions into personal or private affairs and concerns, or should it be limited to intrusions into spatial privacy (unwanted access to our persons and private spaces)?
- Should it include examples?

Q66 Would your answers to questions 5-8 and 11 from chapter 7 differ for the intrusion tort from the answers you gave with respect to the disclosure tort?

Public concern

11.46 We discussed in chapter 6 the defence of legitimate public concern with regard to the disclosure tort. The same defence would be needed for the intrusion tort. However, the focus would be on whether the *intrusion* was for the purpose of uncovering matters of legitimate public concern, rather than on the disclosure of such matters. Spying, prying, and otherwise obtaining unwanted access to a person or a person's private affairs can sometimes be justified in order to reveal

1142 Elizabeth Paton-Simpson "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 U Toronto LJ 305, 321. See also Andrew Jay McClurg "Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places" (1995) 73 NCL Rev 989, 1036-1044; NA Moreham "Privacy in Public Places" (2006) 65 CLJ 606.

misconduct or criminality, identify threats to public health or safety, or for other reasons that are in the public interest. Nicole Moreham therefore suggests that a defence should be available:[1143]

> to any defendant who can show that he or she believed, on reasonable grounds, that the intrusion would reveal information of significant public interest and that there was no other means of obtaining the information realistically available.

11.47 In determining whether legitimate public concern outweighs the need to protect people against privacy intrusions, the considerations may be somewhat different from those that apply to the disclosure tort. First, with regard to freedom of expression, it is the Bill of Rights Act's protection of the freedom to "seek", rather than to "receive, and impart", information that is principally at stake where intrusion is concerned.[1144] To what extent does the freedom to seek information justify intrusions into people's privacy? Few would argue that there should be no restrictions on the methods by which people obtain information about others. It seems clear that some kind of legitimate public interest or concern is needed to justify information-gathering methods that constitute serious interferences with privacy. As with the disclosure tort, there is a question as to whether it would be helpful to give examples of matters of legitimate public concern in a statute. If so, would this list differ in any respects for the intrusion and disclosure torts?

11.48 Secondly, there is the question of whether the statute should require reasonable grounds for belief that a matter is one of legitimate public concern, or whether the test should be an objective one. Here there could be a significant difference between the disclosure and intrusion torts. Where the disclosure tort is concerned, the person publishing private facts could be presumed to be in possession of sufficient information to determine whether or not the publication is about a matter of public concern. In the case of the intrusion tort, however, the defendant may, at the time the intrusion occurred, have reasonably believed that he or she was investigating a matter of public concern, but that belief may prove to have been incorrect. As Eady J observed in the *Mosley* case, the question of whether there was in fact a matter of legitimate public concern "cannot be the test to apply when addressing a decision made prospectively whether or not to install a hidden recording device." In other words, a person cannot be sure whether or not there is a legitimate public concern with regard to something that has not yet happened. In such cases, Eady J suggested, the defendant's conduct could "only be judged by reference to a reasonable apprehension that the public interest would be served."[1145]

1143 NA Moreham "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 LQR 628, 655. See also Lyrissa Barnett Lidsky "Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should do About it" (1998) 73 Tul L Rev 173. Lidsky proposes creating a qualified privilege for the intrusion tort to protect newsgathering in the public interest. The newsgatherer would have to show that he or she had probable cause to believe that the plaintiff's conduct posed a significant threat to the health, safety or financial wellbeing of others, and that the methods used were not substantially more intrusive than necessary to obtain evidence of the wrongdoing.

1144 New Zealand Bill of Rights Act 1990, s 14.

1145 *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), para 142.

11.49 On the other hand, if this test were applied too loosely it could encourage "fishing expeditions" in which intrusive methods were used in the hope that something of public concern might be discovered, regardless of the lack of any strong grounds for believing that the intrusion would be in the public interest. The California Supreme Court has stated that constitutional principle does not give a reporter "general license to intrude in an objectively offensive manner into private places, conversations or matters merely because the reporter thinks he or she may thereby find something that will warrant publication or broadcast."[1146]

11.50 A particular issue for the intrusion tort is how it would deal with intrusions by law enforcement officers. The tort could apply to law enforcement officers who abuse their powers or act unreasonably, or where the intrusion is not undertaken in the course of their duties or in accordance with their powers. There would here be overlap with the "unreasonable search" provisions of the Bill of Rights Act. However, legitimate law enforcement activities would clearly be covered by the defence of public concern.

Q67 If the statute were to give examples of matters of public concern, would the examples for the intrusion tort differ in any respects from those for the disclosure tort?

Q68 With respect to the intrusion tort, should the statute require only reasonable grounds for belief that the intrusion was for the purpose of obtaining information in the public interest or about matters of legitimate public concern, or should the test be an objective one?

Other issues

11.51 Some issues that were raised with respect to the disclosure tort are not relevant to the intrusion tort; for example, the issues relating to false information and identification do not appear to be relevant. However, a number of the other issues that we discussed in relation to the disclosure tort are relevant to the intrusion tort, including the issues of defences, remedies, plaintiffs, and the mental element required for liability. For some of these issues, the answers to the questions we asked in chapter 7 may be the same for both the disclosure and intrusion torts. For others, the answers may differ for the two torts.

11.52 An example of an issue on which the conclusions reached may be different with regard to the intrusion and disclosure torts is whether corporations should be able to sue for invasion of privacy. The argument that privacy is a human value that does not inhere in corporations, which we discussed in chapter 6, is perhaps particularly true with regard to disclosure of private facts. It can be argued that corporations cannot suffer distress or infringement of dignity as a result of the disclosure of facts about them. They may, however, have a right to protection against unreasonable intrusions into their private spaces and concerns. They already have such protection with respect to the state, because the protection against unreasonable search and seizure in section 21 of the Bill of

1146 *Schulman v Group W Productions, Inc* (1998) 955 P 2d 496-497 (Cal Supreme Court) Werdegar J.

Rights Act applies to corporations. It could be argued that they should enjoy similar protection against intrusions by private parties. If, for example, a board meeting was secretly filmed, it is arguable that the intrusion would be on the private affairs of the corporation itself. There could, therefore, be a case for giving the corporation a right to sue, rather than restricting this right to the individual board members.[1147]

Q69 Would your answers to questions 14-16, 19-21 and 23 from chapter 7 differ for the intrusion tort from the answers you gave with respect to the disclosure tort?

Relationship between the intrusion and disclosure torts

11.53 We have indicated above that, in theory, certain features of the disclosure and intrusion torts could differ. This raises the issue of the relationship between the two torts and, indeed, whether they are two distinct torts or whether they make up a single tort of invasion of privacy.

11.54 We have already mentioned the significant area of overlap that is likely to exist between the intrusion and disclosure torts. While they are distinct in theory, in practice many intrusions will be for the purpose of obtaining information that will then be publicised. Nonetheless, there may be cases in which, without an intrusion tort, plaintiffs may be left without an effective remedy for significant intrusions into their privacy. There may be no redress available for intrusions that do not involve publication or disclosure, or there may be no redress against the party who has obtained the information in an intrusive manner when the material is published by a different party. A separate intrusion tort would also allow due consideration to be given to the seriousness of the intrusion itself, rather than simply making it a factor to be taken into account in assessing the offensiveness of publication. We believe, therefore, that the two torts are sufficiently distinct that there is at least an arguable case for introducing an intrusion tort to complement the existing disclosure tort.

11.55 If it were considered desirable to convert the common law tort of disclosure of private facts into a statutory tort, and also to recognise an intrusion tort by statute, it would make sense to include both in the same statute. We invite comment on whether such a statute should treat them as two separate torts or one single tort, and whether it would make any difference.

11.56 The Australian and New South Wales Law Reform Commissions have proposed the creation of a single statutory cause of action for invasion of privacy, which would include a non-exhaustive list of acts or conduct that could constitute an invasion of privacy. Their proposed statutory cause of action would cover both disclosure and intrusion (including surveillance).[1148] The New South Wales Law

1147 For differing views on this question, see the judgments of Lord Woolf MR and Lord Mustill in *R v Broadcasting Standards Commission, Ex p British Broadcasting Corporation* [2001] QB 885, 897, 900-901. See also *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199; New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 193-195.

1148 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007); Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) ch 74.

Reform Commission argued that, in the absence of an existing body of jurisprudence like that on which Prosser based his classification of the United States privacy torts, any attempt to categorise privacy invasions and create distinct causes of action was likely to be arbitrary. It also ran the risk of leaving some claims warranting redress falling between the cracks.[1149] The Law Reform Commission of Hong Kong, by contrast, considered that a general tort of invasion of privacy "would make the law uncertain and difficult to enforce", and preferred the creation of "one or more specific torts of invasion of privacy which clearly define the act, conduct and/or publication" which breaches reasonable expectations of privacy. They recommended the creation of both an intrusion and a disclosure tort.[1150] Treating disclosure and intrusion as two distinct torts might give greater scope for recognising differences between them on some of the points discussed above.

Q70 What do you think should be the relationship between the disclosure and intrusion torts if both were to be put on a statutory basis?

Dealing with intrusion outside the courts

11.57 One final option would be to introduce a mechanism for dealing with privacy intrusions that is at a lower level and therefore more accessible than a tort that can only be pursued through the courts. For example, the Privacy Commissioner could be given jurisdiction to accept complaints with respect to intrusion, regardless of whether the intrusion involves collection or use of personal information. Such a jurisdiction could build on the Commissioner's existing experience with handling complaints under information privacy principle 4. We have already discussed in the previous chapters the possibility of giving the Privacy Commissioner an increased role in relation to surveillance. There could be a case for giving the Commissioner jurisdiction in relation to intrusion more generally, although this would extend the scope of the Act by introducing a principle or principles which are not "information privacy" principles. However, it would probably not make sense for intrusion to be dealt with at a lower level while disclosure is still handled through the courts as a fully-fledged tort. Our feeling is that the same approach should be taken to both types of privacy invasion. We would welcome comments on the issue of whether a lower-level approach would be preferable to a tort and, if so, what form this might take. We also note that a lower-level option could co-exist with a right to bring a civil action in the courts.

Q71 Should there be a mechanism for dealing with intrusion at a lower level as an alternative to proceeding through the courts? If so, what form should this take? Should intrusion and disclosure both be dealt with at the same level?

1149 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 157-158.

1150 Law Reform Commission of Hong Kong *Civil Liability for Invasion of Privacy: Report* (2004) 107, 139, 165.

Chapter 12
Specific sectors

12.1 The preceding chapters in this Part have looked at how surveillance and other forms of intrusion might be controlled by laws of general application. In this chapter we look at surveillance and intrusion issues in three specific sectors: the media, employment, and the private investigation industry. We discuss these sectors in more detail for two reasons. First, they raise particular challenges in terms of balancing privacy with legitimate public and business interests. Secondly, they are already governed by laws or regulatory mechanisms that are particular to each sector, and that place some controls on the use of surveillance and other intrusions. We provide some background on the use of surveillance and other forms of intrusion in each sector, discuss the application of the current legal framework, and look at privacy issues and options for reform.

MEDIA

Background

The media and surveillance or other intrusions

12.2 Our definition of surveillance in chapter 8 is sufficiently broad that it would cover much of the activity of the print and broadcast media. It is not our intention, however, to bring the bulk of the media's everyday activities in gathering news and producing entertainment programmes within any new legal framework for regulating surveillance. At the same time, there are occasions when the methods used by the media, or the focus on monitoring particular individuals, could be considered to amount to a form of surveillance. It is possible that some media activity could be caught by any new laws dealing with surveillance and intrusion, unless specific exemptions or defences for the media are provided.

12.3 A number of scenarios in chapters 9 and 11 involved the media as the party undertaking surveillance or other intrusions.[1151] Other scenarios involved the media as disseminators of information obtained in an intrusive manner by others.[1152] Examples of media activity that could be considered to be forms of surveillance or intrusion include:

- the use of hidden cameras or microphones to record people;
- filming or taking photographs of people in their homes or other private places without consent;

1151 Chapter 9, Scenarios 5, 6, 13 and 16; chapter 11, Scenarios 1 and 7.

1152 Chapter 9, Scenarios 7 and 8(a); chapter 11, Scenario 4.

- the use of telescopic lenses to photograph targeted individuals in public places without their knowledge;
- persistently following people or waiting outside their homes in order to observe their activities or obtain interviews with them;
- obtaining information by deception; and
- obtaining information by other intrusive methods, such as those discussed in the scenarios in chapter 11.

The Commission would like to hear from submitters whether media activities such as these should be covered by any new legal regimes for surveillance and intrusion that might result from our Review, or whether they should be excluded from the coverage of such regimes.

12.4 In addition to material that they obtain themselves, the media sometimes use material obtained through surveillance by others. Both the print and broadcast media often make use of CCTV footage relating to crimes. The release of such images to the media by the Police can assist with identifying suspects, but other uses of CCTV footage by the media could be more questionable. The CCTV Code of Practice issued by the United Kingdom Information Commissioner states that "it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes".[1153] Another source of images for the media is the growing phenomenon of "citizen journalism", with ordinary people sending in photographs or video footage of notable events, often taken with cellphone cameras. The capturing of such images is generally opportunistic rather than planned, but citizen journalists may increasingly engage in more systematic gathering of material in future. They may be less constrained than the established broadcasters by privacy concerns, particularly if they upload their images directly to the internet.

The media environment

12.5 The nature of the media in New Zealand, as in all developed countries, is changing dramatically. The convergence of print and broadcast media via the internet has altered the traditional competitive boundaries between media organisations in this country. As Bill Rosenberg notes, "The line between the internet and other publishing and communications is increasingly blurred."[1154] Blogs, social networking sites, video-sharing sites such as YouTube, and online trading sites like Trade Me are challenging the dominance of the traditional media, leading to a decline in market share and advertising revenue for the print and broadcast media. User-generated content on such sites, created by members of the public without editorial intervention, is now competing with content produced by the traditional media.

12.6 At the same time, newspapers, magazines, and television and radio stations now have their own websites. They regularly place on these sites not only the content of their printed stories or broadcasts, but also additional material, including video and audio. For example, when the *News of the World* in the United Kingdom published a story about Max Mosley's involvement in a private sadomasochistic

1153 *CCTV Code of Practice* (Information Commissioner's Office, Wilmslow, 2008) 13.

1154 Bill Rosenberg "News Media Ownership in New Zealand" (13 September 2008) 27, available at http://canterbury.cyberplace.co.nz/community/CAFCA.

party, it also placed secretly-filmed footage of the party on its website. The website footage attracted some 3.5 million hits.[1155] The inclusion of audiovisual material on print media websites, and written content on broadcasters' websites, also blurs the lines between the print and broadcast media.

12.7 One consequence of competition within an increasingly converged media market may be a growing emphasis in the traditional media on entertainment, celebrity gossip and other "soft" news.[1156] Such news is both popular and often relatively cheap to obtain at a time when commercial pressures are leading media companies (particularly in the print media) to cut staff. Journalist Simon Collins comments that reduced journalistic resources:[1157]

> have been increasingly diverted from serious public issues to private celebrity gossip and entertainment … News judgments are being made in response to panels of readers emailing in to comment on each day's stories, and by the number of website hits on each story.

In New Zealand, as elsewhere, it seems that "the stories that generate the most hits online are often trashy/sleazy ones".[1158] Moreover, the unprecedented publication of personal and intimate content on social networking sites has arguably further blurred the public/private divide for mainstream news organisations, which increasingly rely on such sites as research sources.

12.8 There are a number of features of the current media environment that could have implications for privacy. First, commercial pressures to report on celebrity gossip, scandal and dramatic events such as accidents or murders may lead to the use of increasingly intrusive methods of gathering material, and more extensive prying into people's private lives. Secondly, the line between entertainment and news is becoming even more difficult to define clearly. This raises the question of the extent to which the media should be able to rely on freedom of expression arguments in privacy cases where the subject matter does not clearly relate to matters of public concern. Thirdly, as the traditional media become less dominant, privacy intrusions will increasingly be carried out for the purpose of putting material on websites rather than printing or broadcasting it. Internet content is, however, largely unregulated.

Regulation of surveillance and other intrusions by the media

12.9 As we discussed in chapter 3, the media's news activities are excluded from the coverage of the Privacy Act 1993. We will consider this exclusion as part of our review of the Privacy Act in Stage 4 of the Commission's Review. Complaints about breaches of privacy by the media can be made to the Broadcasting Standards Authority (BSA), Press Council or Advertising Standards Authority (ASA). There is no body with specific responsibility for regulating content on the

1155 Frances Gibb "Max Mosley Opens New Front in the Battle for Privacy" (25 July 2008) *The Times* www.timesonline.co.uk (accessed 26 July 2008).

1156 House of Lords, Select Committee on Communications "The Ownership of the News. Volume I: Report" (HL 122-I, 2008) 18.

1157 Simon Collins "Commercial Pressures on Journalism" (speech to Journalism Matters summit, Wellington, 11-12 August 2007), available at www.ourmedia.org.nz (accessed 23 December 2008).

1158 An Australian journalist quoted in Media, Entertainment & Arts Alliance *Life in the Clickstream: The Future of Journalism* (Redfern (NSW), 2008) 15.

internet. The Press Council accepts complaints about material on the websites of the print media, and the ASA covers online advertising, but the BSA's jurisdiction does not extend to broadcasters' websites.[1159] The current regulatory review of digital broadcasting is examining options for regulating broadcasting and telecommunications, including the internet.[1160]

12.10 Convergence and the blurring of boundaries between different media (including the internet) raise significant challenges for media regulation, as well as issues about consistency between different regulatory regimes. The Review of the Press Council noted the increasingly arbitrary nature of the jurisdictional differences between the print and broadcast media, and the difficulties of extending any system of content regulation to include general coverage of the internet.[1161] These issues are beyond the scope of our Review, but we note that they have implications for consistency of privacy protection across different media.

12.11 The media are also covered by the general civil and criminal law, such as the laws of trespass and breach of confidence, and the prohibition on interception of private communications.[1162] These laws do not have specific exemptions or defences for the media, although in some cases the media may be able to rely on general defences. For example, the Harassment Act 1997 (section 17) provides for a defence where a respondent proves that a specified act was done for a lawful purpose. "Lawful purpose" is not defined in the Act, but the intention of the defence is to protect legitimate activity such as picketing, protesting and newsgathering.[1163]

12.12 The BSA Standards that are most relevant to surveillance and intrusion are those concerning Fairness and Privacy.[1164] In relation to the Privacy Standards, we have discussed in chapters 3, 9 and 11 the BSA's Privacy Principle 3, which concerns intrusion. Also relevant are the guidelines to the Fairness Standard for free-to-air television, which state that information and pictures should not be

1159 *Davies v TVNZ* (31 March 2005) Broadcasting Standards Authority 2004-207: content downloaded from a broadcaster's website does not fall within the meaning of "broadcasting" in the Broadcasting Act 1989. The BSA may, however, have jurisdiction with regard to material being streamed live over a broadcaster's website.

1160 Documents relating to the review of digital broadcasting are currently available on the Ministry of Culture and Heritage website www.mch.govt.nz (accessed 31 October 2008).

1161 Ian Barker and Lewis Evans *Review of the New Zealand Press Council* (New Zealand Press Council, Wellington, 2007) 14-15, 18-19.

1162 See generally John Burrows and Ursula Cheer *Media Law in New Zealand* (Oxford University Press, South Melbourne, 2005); Steven Price *Media Minefield: A Journalists' Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) chs 18-22.

1163 Ministry of Justice "Memorandum to Cabinet Social Policy Committee: Proposals to give Greater Protection to Victims of Harassment" (June 1996) 7, cited in John Burrows and Ursula Cheer *Media Law in New Zealand* (Oxford University Press, South Melbourne, 2005) 282 (n 380).

1164 Broadcasting Standards Authority *Free to Air Television Code of Broadcasting Practice*, Standards 3 and 6; *Radio Code of Broadcasting Practice*, Standards 3 and 5.

gathered through misrepresentation or deception, "except as required in the public interest when the material cannot be gathered by other means".[1165] This provides a basis for complaints in cases of covert filming and audio-recording.

12.13 BSA decisions under both the Fairness and Privacy standards have indicated that broadcasters must be very careful about using covert tactics such as hidden cameras or microphones to obtain material that is broadcast. The BSA has stated that there is "a presumption that hidden filming will be unfair unless there are overriding public interest factors".[1166] This is because the use of hidden cameras prevents those filmed from withholding comment, can create the impression that dishonesty or misconduct is being uncovered, and can produce footage that is highly prejudicial, private or intimate in nature.[1167] The BSA has also found that the use of hidden cameras will usually be an intentional interference with solitude or seclusion "in the nature of prying" for the purposes of Privacy Principle 3.[1168] According to media law specialist Steven Price, BSA decisions indicate that before material obtained by the use of hidden cameras is broadcast, the broadcaster must be satisfied that there is a legitimate and strong public interest in the broadcast that clearly outweighs individual privacy rights; that prima facie evidence exists of misconduct by the subjects of the filming; and that there is no other reasonable way to obtain the information. The persons filmed must also be given a chance to understand and respond to the recorded material.[1169]

12.14 The Press Council has a Privacy Principle, which we have set out in chapter 3. It also has a principle relating to "Subterfuge", which states that: "Editors should generally not sanction misrepresentation, deceit or subterfuge to obtain information for publication unless there is a clear case of public interest and the information cannot be obtained in any other way." As with the BSA's Fairness Standard, this would appear to rule out the use of covert recording devices, except where there is a clear public interest in information obtained in this way. The Press Council does not seem to have ruled on any complaints concerning the use of hidden cameras or microphones.

12.15 It is also worth mentioning that media organisations are governed by their own internal policies and protocols, and that the Engineering, Printing and Manufacturing Union (EPMU) has a Code of Ethics for its journalist members. This Code states, among other things, that journalists should use fair and honest means to obtain material; should identify themselves and their employers before obtaining interviews for broadcast or publication; and should respect private grief and personal privacy. A breach of the Code may give rise to disciplinary procedures under the EPMU's Rules.[1170]

1165 Broadcasting Standards Authority *Free to Air Television Code of Broadcasting Practice*, Guideline 6c. See also *Radio Code of Broadcasting Practice*, Guideline 5a, which states that telephone conversations should not be recorded or broadcast for radio programmes without advising the subject that the conversation is being, or may be, recorded or broadcast (although "Exceptions may apply depending on the context of the broadcast, including the legitimate use of humour.")

1166 *OK Gift Shop Ltd v TV3* (4 May 2005) Broadcasting Standards Authority 2004-199, para 34.

1167 Steven Price *Media Minefield: A Journalists' Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 70.

1168 See for example *O'Connell v TVWorks* (25 June 2008) Broadcasting Standards Authority 2007-067, para 47.

1169 Steven Price *Media Minefield: A Journalists' Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 70-71, and generally 70-72, 116, 117-121.

1170 Engineering, Printing and Manufacturing Union "Journalist Code of Ethics", available at www.epmu.org.nz.

Issues and reform options

12.16 Probably the most intrusive interferences with privacy by the media are those that involve the use of hidden cameras, hidden microphones and other covert devices. Such tactics may be justified where a story is clearly in the public interest and there is no other way of obtaining the information. Perhaps the best-known New Zealand example is the "20/20" television programme's investigation of Christchurch doctor Morgan Fahey, who was running for mayor of Christchurch. A number of Fahey's patients had accused him of sexual abuse, but he denied the allegations, and the Police considered that there was insufficient evidence to prosecute him. "20/20" arranged for one of his former patients, equipped with a hidden camera, to make an appointment to see him. The patient accused him of abusing her, and recorded his reaction, which was damning. Fahey was subsequently convicted of rape and other sexual offences. The BSA did not uphold complaints on privacy and fairness grounds about the "20/20" programme's use of hidden camera footage because there was a legitimate public interest in the story, and because the information could not have been obtained in any other way.[1171] On the other hand, hidden cameras can be used for "fishing expeditions" in cases where there is no reason to suspect wrongdoing.[1172] They can also be used simply to provide dramatic footage, when the information could have been obtained by other, less intrusive means.

12.17 While the use of hidden cameras and microphones may raise the most serious privacy issues, it is filming or photographing in or from a public place that is the area of greatest uncertainty for the media.[1173] Media representatives have told the Commission that the use of hidden cameras is rare in New Zealand, and is governed by very clear internal protocols. By contrast, they reported that issues about filming in or from public places arise every day, and that television crews are often uncertain about what they can and cannot film. Filming in public is said to be becoming increasingly difficult, because the standards imposed by the BSA are becoming harder to meet.[1174] Similar issues arise for print media photographers. In general, both the BSA and the Press Council have said that openly filming or photographing people in public places does not intrude on their privacy. However, even in public places some filming or other media activity may constitute an intrusion, as the BSA has recognised in a qualification to its public places exemption for individuals who are "particularly vulnerable". There is also a grey area around filming or long-lens photography of people on private property when the camera operator is in a public place. BSA decisions have been somewhat inconsistent with regard to filming people on private property from a public place.

12.18 Another issue is that there is a tension between privacy and newsgathering with regard to people who are involuntarily experiencing traumatic events in public places. One view is that such people are particularly vulnerable, and that in some

1171 *DeHart and others v TV3 Network Services* (10 August 2000) Broadcasting Standards Authority 2000-108 to 113; see also *TV3 Network Services v Fahey* [1999] 2 NZLR 129 (CA).

1172 See for example *O'Connell v TV Works Ltd* (25 June 2008) Broadcasting Standards Authority 2007-067.

1173 Relevant BSA and Press Council decisions are discussed in Steven Price *Media Minefield: A Journalists' Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) 112-113, 120-121, 196, 202.

1174 Law Commission meeting with media industry representatives, 3 July 2007.

cases they should be exceptions to the general rule that people (including the media) are free to film in public places.[1175] However, traumatic events such as accidents or shootings that occur in public places are also highly newsworthy, especially if dramatic footage can be obtained.

12.19 One area of possible uncertainty that is yet to be tested in New Zealand concerns the application of the Harassment Act 1997 to the media. The Act has not so far been used to restrain the media in New Zealand, in contrast to the United Kingdom. Scenarios 5 and 6 in chapter 9 illustrated some of the complexities of applying the Act to the media, particularly where multiple reporters and camerapeople are involved. It is important to note that the Act was never intended to deal with issues of media harassment. Rather, it was aimed at stalking by individuals and intimidation by gangs.[1176] Nonetheless, there is nothing in the Act preventing its use to restrain certain kinds of newsgathering by the media, apart from the defence of lawful purpose. When the Bill was before the select committee, the Commonwealth Press Union raised concerns about possible use of the civil regime against the media, but it was considered that the legislation provided adequate safeguards.[1177] The question is whether the Act provides sufficient protection against harassment by the media, or whether on the other hand it goes too far in providing a mechanism that could be used to unduly restrain the media. We have put forward in chapters 9 and 11 some options for changes to the Act, and if these were to go ahead the implications for the media would need to be carefully considered.

12.20 The gathering of information (including images) by the media plays a vital role in informing people about issues of public importance, and about the lives of their fellow citizens and communities. It is also integral to freedom of expression, which is protected by section 14 of the New Zealand Bill of Rights Act 1990. Any restriction on information-gathering by the media will be a limitation on the "freedom to seek, receive, and impart information and opinions", and will therefore need to be reasonable, demonstrably justified and prescribed by law.[1178] The majority of the Court of Appeal in *Hosking* held that privacy is a value that can, in some circumstances, outweigh freedom of expression and justifiably limit that freedom.[1179] Moreover, protection from surveillance and intrusion also plays a part in protecting freedom of expression, since people will often feel constrained from expressing themselves freely if they know or suspect that they are under observation. The balancing act involved in protecting media freedom while also protecting people against unreasonable intrusions by the media is a delicate and, at times, difficult one.

1175 NA Moreham "Privacy in Public Places" (2006) 65 CLJ 606, 623-627, 634-635. Moreham acknowledges the need for a public interest defence for newsgathering.

1176 DAM Graham (Minister of Justice) (20 November 1997) 565 NZPD 5534; Jane Mountfort "The Civil Provisions of the Harassment Act 1997: A Worrying Area of Legislation?" (2001) 32 VUWLR 999, 1011-1012.

1177 John Burrows and Ursula Cheer *Media Law in New Zealand* (Oxford University Press, South Melbourne, 2005) 281; see also the comments of Pansy Wong and Patricia Schnauer (20 November 1997) 565 NZPD 5540, 5543.

1178 New Zealand Bill of Rights Act 1990, s 5.

1179 *Hosking v Runting* [2005] 1 NZLR 1, paras 129-135, 230-237 (CA) Gault P and Blanchard J; Tipping J.

12.21 When considering the application to the media of the current or future legal and regulatory framework for dealing with surveillance and other intrusions, there are two main questions:

- Does the current framework of content regulation by the BSA and the Press Council provide adequate protection against intrusions by the media? Alternatively, does it go too far in limiting media freedom?
- To what extent should the media be exempted from any criminal offences or civil liability in relation to surveillance and other intrusions, and what form should any such exemptions take?

12.22 With regard to the second of these questions, there are a number of possible options. The law could:

(a) provide no exceptions or defences either to the media or to most other members of the public, as in the current interception offences under the Crimes Act 1961;

(b) provide a general defence of legitimate public interest or public concern, as in breach of confidence and the tort of breach of privacy by publication of private facts;

(c) provide a general defence of "lawful purpose", as in the Harassment Act 1997;

(d) provide a public interest or lawful purpose defence which further defines or particularises these terms, and expressly includes media activity; or

(e) expressly state that it does not apply to the media, either generally or in their news activities, as in the Privacy Act 1993.

Of these various options, only (d) and (e) would apply specifically to the media, but (b) and (c) could also be relied on by the media in many cases. Each of these options will be more appropriate to some legal frameworks than others. We would welcome comments on how they might apply to the possible frameworks for dealing with surveillance and other intrusions discussed in earlier chapters.

12.23 An additional question is whether any exemptions or defences for the media should apply generally or only to the media's news activities. Surveillance and other intrusive methods may be used by the media for reasons of clear public interest, such as exposing serious wrongdoing. They may also be undertaken for reasons of entertainment: for example, exposing the private life of a celebrity, or gathering "humorous" footage of people engaged in embarrassing activities. The rise of "reality television" programmes and the growing importance of "soft news" such as celebrity gossip may have blurred the line between reporting and entertainment. If any media exemptions from laws protecting privacy are to protect only the media's newsgathering activities, how are those activities to be defined and distinguished from entertainment? As we noted in chapter 3, the news media exclusion from the Privacy Act has been interpreted broadly.

Q72 Should the media be subject to any greater, or lesser, legal restrictions concerning surveillance and other intrusions than other members of the public?

Q73 Does the current framework of content regulation by the BSA and the Press Council provide adequate protection against intrusions by the media? Alternatively, does it go too far in limiting media freedom?

Q74 To what extent should the media be exempted from laws dealing with surveillance and other intrusions (either current laws, or options for reform discussed in this issues paper)?

Q75 What form should any exemptions for the media take? Should they be restricted to newsgathering, and if so, how should newsgathering be distinguished from entertainment?

WORKPLACE

Background

12.24 Surveillance in the workplace can take a number of forms, such as the use of cameras, audio recording, and installation of tracking devices in vehicles. Computer monitoring of employees, such as logging their keystrokes, reading their emails, and tracking their internet use, could also be considered to constitute surveillance.[1180] Other actions by employers, such as requiring employees to undergo drug testing or to submit to searches of their bags, lockers or vehicles, could fall within the broader category of intrusion discussed in chapter 11. We discussed a number of hypothetical examples of workplace monitoring, and how they might be covered by existing law, in *Privacy: Concepts and Issues*.[1181] Some workplace privacy issues, such as those relating to employee records, will be considered when we review the Privacy Act 1993 in Stage 4 of the Commission's Review.

12.25 Broadly speaking, surveillance and other forms of monitoring are used by employers to increase productivity and efficiency, to protect their property, and to avoid liability.[1182] More specific purposes for surveillance in the workplace include:

- detection of theft or serious misconduct (including harassment or offensive behaviour towards co-workers or customers);

1180 David Maida "Who Watches You at Work?" (28 February 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 23 March 2007); Brooke Donovan "Big Brother in the Office" (26 January 2008) *New Zealand Herald* Auckland B6.

1181 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 214-216. For further hypothetical scenarios, and discussion of how the Privacy Act applies to such cases, see Privacy Commissioner *Privacy at Work: A Guide to the Privacy Act for Employers and Employees* (Office of the Privacy Commissioner, Wellington, 2008).

1182 Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65, 71.

- performance monitoring and management (including training and development);
- monitoring use of company equipment;
- health and safety monitoring;
- accident investigation; and
- keeping a record of transactions.

12.26 Some forms of surveillance may be directed both at employees and at customers: for example, video cameras in shops could detect shoplifting as well as employee misconduct, and recording of phone calls between customers and call centre staff could be used to establish whether the customer or the staff member was at fault in cases of customer complaints.

12.27 Covert surveillance is sometimes used in the workplace, particularly when suspected theft by employees is being investigated, but much workplace surveillance is overt. The overt nature of the surveillance may take different forms: it may be obvious that cameras or other devices are operating, notices may be posted stating that surveillance is taking place, or surveillance practices may be detailed in corporate policies. Examples of overt surveillance of employees include:

- the use of cameras to record or monitor workplaces for reasons of security, health and safety, and protection of property;
- recording of phone calls between employees and customers; and
- use of Global Positioning System devices to monitor the movement of vehicles such as taxis or trucking fleets.

12.28 In addition to surveillance that takes place while employees are at work (whether in a fixed location such as an office or shop, or while employees are travelling for work-related reasons), employers may sometimes monitor employees when they are at home or off duty. This may be done using the services of a private investigator. For example, workers could be put under surveillance to see whether they have genuine reasons for taking extended sick leave, or whether they are making inappropriate personal use of company equipment. It is possible that monitoring of employees in their homes, or in relation to their off-duty conduct, could increase in future for two reasons. First, the lines between work and home may become increasingly blurred as technology makes it easier for people to work at home. Secondly, public image, which may be adversely affected by out-of-work activities that bring a company into disrepute, is increasingly important to businesses, particularly in the growing services sector.[1183]

12.29 The extent to which there is a reasonable expectation of privacy in the workplace is a somewhat vexed question. Workplaces are not easily categorised as either public or private places. Many workplaces are not public in the sense of being open to entry by the general public, but neither are they as private as a person's home: employees can expect to be observed by their co-workers, as well as by employers. Many people also work in environments where they interact with, and can be observed by, the general public. However, even in such "public" workplaces, there are areas such as storerooms, staff bathrooms and staff canteens that are not open to the public.

1183 Paul Roth "Privacy in the Workplace" (Paper for Privacy Issues Forum, Wellington, 27 August 2008) 1.

12.30 The main arguments in favour of relatively limited privacy rights in the workplace are that:[1184]

- Workers enter into employment agreements voluntarily, and can be assumed to have waived at least some of their privacy rights by entering into such agreements. If they do not like the conditions of work, they are free to seek work elsewhere.
- Employers have a right to protect their property. The employer owns or controls the workplace and the equipment used to carry out the work; therefore, the employer has a right to monitor what happens in the workplace and how the equipment is used.

12.31 The main counter-arguments in favour of workers' privacy rights are that:

- 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.

12.32 Employees do have rights to privacy while at work, but they must be balanced against the rights of employers and co-workers, and they will be limited by the nature of the workplace environment. An employee's reasonable expectations of privacy will also vary depending on contextual factors such as his or her role, location and behaviour, and whether there has been proper consultation and notice about any use of overt surveillance or other intrusions.[1185]

Legal controls on intrusion and surveillance in the workplace

12.33 Workplace surveillance is governed by the Privacy Act 1993 and by the general provisions of the civil and criminal law discussed in chapter 2. In addition, it is governed by aspects of employment law, such as procedural protections and obligations of trust, confidence and good faith.[1186]

12.34 A number of commentators have suggested that the law currently favours employers where workplace privacy is concerned, and in particular that the Privacy Act has done little to protect employee privacy.[1187] In addition to the

1184 The arguments on both sides are summarised by Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65, 69-71.

1185 The International Labour Organisation has developed a code of practice which provides some general guidelines on workplace monitoring, including surveillance: International Labour Organisation *Protection of Workers' Personal Data: An ILO Code of Practice* (International Labour Office, Geneva, 1997) para 6.14.

1186 See generally Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65; Paul Roth "Privacy in the Workplace" (Paper for Privacy Issues Forum, Wellington, 27 August 2008); Department of Labour *Big Brother Goes to Work: Video Surveillance in the Workplace* ("Themes in Employment Law", October 2005); Employers and Manufacturers Association (Northern) *Surveillance* and *Tape Recordings* ("A-Z of Employing – A Managers Guide", January and June 2007).

1187 Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65, 89-90; Paul Roth "Privacy in the Workplace" (Paper for Privacy Issues Forum, Wellington, 27 August 2008); "Interviews May Go Genetic" (27 September 2008) *Dominion Post* Wellington G3.

general uncertainties surrounding the Act's application to surveillance, which we have discussed in previous chapters, it has been argued that the Privacy Commissioner's opinions have tended to afford employers a significant degree of discretion with regard to surveillance and other intrusions, such as bag searches.[1188] There have, however, been cases in which the Commissioner has formed the opinion that an employer's actions were in breach of the Act.[1189] Moreover, it is likely that the existence of the Act causes employers to think twice before intruding unreasonably into their employees' privacy.[1190] The Privacy Act may also influence employment law. Employers are required to act in a fair and reasonable manner, and the Privacy Act can be taken as representing community standards about what is fair and reasonable where protection of workers' informational privacy is concerned.[1191]

12.35 It is an implied term of all employment agreements that the parties have mutual obligations of trust, confidence and good faith.[1192] The courts have not held that surveillance of employees is inherently contrary to these obligations, but in some circumstances it might be. Employment law also provides protections where evidence obtained through surveillance is used as the basis for dismissing an employee. Dismissals must be fair procedurally as well as substantively, and there are two important respects in which dismissals based on the evidence of surveillance may be deemed procedurally defective. First, the surveillance evidence may not in fact be sufficiently compelling to justify dismissal on grounds of misconduct. Secondly, the dismissal will be unfair if the employee has not been given a proper opportunity to comment on the surveillance evidence.[1193]

Issues and reform options

12.36 The key question in relation to surveillance and other forms of intrusion in employment is whether the existing law achieves the proper balance between the interests of employers and employees. Rebecca Britton argues that "The law as it currently stands appears to favour the interests of employers over the privacy rights of employees." She identifies a number of specific areas in which reform is called for, proposing that there is a need for:

- regulations governing bodily intrusions such as drug and alcohol testing;

1188 Paul Roth "Privacy in the Workplace" (Paper for Privacy Issues Forum, Wellington, 27 August 2008); Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, 2008) PVA.6.7(e), EPM.3.5.

1189 See for example *Employee Objects to Employer's Hidden Tape Recording in Theft Investigation* [2001] NZPrivCmr 6 – Case Note 16479.

1190 See the advice about the application of the Act in Employers and Manufacturers Association (Northern) *Surveillance* ("A-Z of Employing – A Managers Guide", January 2007) and Privacy Commissioner *Privacy at Work: A Guide to the Privacy Act for Employers and Employees* (Office of the Privacy Commissioner, Wellington, 2008).

1191 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, 2008) EMP.3; Department of Labour *Big Brother Goes to Work: Video Surveillance in the Workplace* ("Themes in Employment Law", October 2005) IV.A; *NZ Amalgamated Engineering Printing and Manufacturing Union Inc v Air New Zealand Ltd* [2004] 1 ERNZ 614, para 221 (Emp Ct).

1192 See Department of Labour *Big Brother Goes to Work: Video Surveillance in the Workplace* ("Themes in Employment Law", October 2005) II; Employers and Manufacturers Association (Northern) *Surveillance* ("A-Z of Employing – A Managers Guide", January 2007) 7-8; Employers and Manufacturers Association (Northern) *Tape Recordings* ("A-Z of Employing – A Managers Guide", June 2007) 4.

1193 Department of Labour *Big Brother Goes to Work: Video Surveillance in the Workplace* ("Themes in Employment Law", October 2005) III.

- guidelines as to appropriate use of surveillance due to the apparent limitations of the Privacy Act in this area;
- restrictions on monitoring employees' off-duty conduct; and
- laws which are sufficiently flexible to adapt to future technological developments.[1194]

This is, however, only one view, and we welcome submissions on whether there is a need for reform in this area.

12.37 If it is considered that reform is needed, one option would be specific legislation dealing with workplace surveillance. In *Privacy: Concepts and Issues*, we reviewed legal developments in Australia with regard to workplace surveillance and privacy.[1195] The most comprehensive existing statute dealing with this topic in Australia is the Workplace Surveillance Act 2005 (NSW). This Act provides for notification to employees where overt camera, computer or tracking surveillance is carried out. Where an employer wishes to carry out covert surveillance, authorisation must be obtained from a magistrate. Surveillance of employees in bathrooms, change rooms and toilets is prohibited, as are some types of surveillance of employees when they are not at work. A much more comprehensive regime for dealing with workplace privacy was proposed by the Victorian Law Reform Commission (VLRC).[1196] The VLRC's report has not been implemented in full, but one of their recommendations was implemented by the Surveillance Devices (Workplace Privacy) Act 2006 (Vic), which introduced a prohibition on the use of optical surveillance or listening devices in toilets, washrooms, change rooms and lactation rooms.

12.38 Another option would be to develop a code or codes dealing with workplace surveillance or workplace privacy more generally. There are several possibilities for developing such codes:

- The Privacy Commissioner could develop a code under Part 6 of the Privacy Act 1993, specifying how the information privacy principles apply to workplace surveillance.
- A code of employment practice could be promulgated under section 100A of the Employment Relations Act 2000, providing guidance on the application of the Act in relation to workplace surveillance or privacy.
- Industries could develop codes through negotiation between employer and employee representatives, together with self-regulatory enforcement mechanisms.

1194 Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65, 89-90.

1195 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 216-218. The Privacy Act 1988 (Cth) does not cover workplace privacy in Australia as comprehensively as does the Privacy Act 1993 in New Zealand. This is because of exclusions from the Privacy Act 1988 (Cth) in relation to employee records and small businesses.

1196 See Victorian Law Reform Commission *Workplace Privacy: Final Report* (VLRC, Melbourne, 2005), and our summary of this report in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 216-217.

12.39 Any legal reform in relation to workplace surveillance and privacy is likely to be complex, involving as it does a number of competing interests and different areas of law. If, following submissions on this issues paper, the Commission considers that legal reform is needed in this area, it might need to be the subject of a separate study, involving further research and consultation.

Q76 Are the issues relating to surveillance and other forms of intrusion in employment significantly different from issues in other areas? If so, how?

Q77 Does the current legal framework achieve an appropriate balance between the interests of employers and employees with regard to surveillance and other forms of intrusion? If not, in what areas is reform needed to achieve an appropriate balance?

Q78 Should there be a specific statute governing workplace surveillance? If so, what areas should it cover?

Q79 Should there be a code governing workplace surveillance or workplace privacy generally? If so, what areas should it cover, and what mechanism should be used to introduce it?

PRIVATE INVESTIGATORS

Background

12.40 To operate as a private investigator in New Zealand, a person must hold a licence under the Private Investigators and Security Guards Act 1974. In 2007/08 there were 161 people holding private investigators' licences, many of them ex-Police officers. Licensed private investigators may employ "responsible employees" to seek or supply information on their behalf, and such employees must be approved in accordance with the provisions of the Act. There were 311 responsible employees of private investigators in 2007/08.[1197]

12.41 The Act defines a private investigator as a person who is paid by a client to obtain certain types of information that is not on the public record, including information about the character, actions, financial position, business, identity or whereabouts of any person. Certain activities, such as newsgathering, academic research and debt collection, are specifically excluded from the

1197 For background on the private investigation industry see Joanne Black "Trevor Morley: Private Investigator" (21-27 October 2006) *New Zealand Listener* www.listener.co.nz (accessed 16 October 2006); Phil Taylor "Spying OK in the Eyes of the Law" (5 April 2008) *New Zealand Herald* Auckland B6; Trevor Morley "The Role of the Private Investigator in Modern Criminal Investigations" (paper presented at Privacy Issues Forum, Wellington, 27 August 2008). Figures on the numbers of private investigators and responsible employees were supplied by the Registrar of Private Investigators and Security Guards.

definition.[1198] The Act does not apply to "in-house" investigators who are employees of the Accident Compensation Commission or of a bank or other commercial enterprise.[1199]

12.42 Private investigators are employed to do a variety of tasks, including investigating insurance or accident compensation claim fraud;[1200] gathering evidence for criminal or civil cases; carrying out debugging and other electronic counter-measures; investigating employee theft or misconduct; locating missing persons; serving documents; and doing background checks. Finding evidence of adultery is no longer such an important part of the work of private investigators as it was when the Act was passed, due to the move to no-fault divorce. Nonetheless, some private investigation work still involves domestic matters, such as investigating suspected infidelity by partners, or drug use by children.

12.43 Private investigators may employ a range of methods to obtain information, including use of surveillance devices and covert human intelligence. Covert human intelligence can include secretly following or watching the subject without using devices, or obtaining information by misleading conduct such as assuming a false identity or failing to disclose the investigator's true purpose for seeking information. For example, in 2007 there was some controversy over the use by a private investigation firm of paid informants within a protest group.[1201]

12.44 Following a review of the Private Investigators and Security Guards Act 1974, the Government introduced the Private Security Personnel and Private Investigators Bill in September 2008. The Bill, which would replace the current Act, would continue to require private investigators to be licensed, and their responsible employees to obtain certificates of approval. It also retains the existing restrictions on audio and visual recording by private investigators.[1202] A further review of the legislation as it applies to private investigators has been undertaken by the Ministry of Justice. This review looked at what legal obligations, if any, private investigators and their responsible employees should have to avoid engaging in misleading conduct to obtain information, and to ensure that information gathered for clients is not used for illegal purposes or for intimidation. The Ministry produced a discussion document and called for public submissions on these issues.[1203] The outcome of the Ministry's review had not been made public by the time the Law Commission's issues paper went to press.

12.45 In addition to the further review by the Ministry of Justice, Cabinet agreed that the Law Commission should consider issues relating to the use of surveillance by private investigators as part of the Commission's Review of Privacy.

1198 Private Investigators and Security Guards Act 1974, s 3.

1199 Trevor Morley "The Role of the Private Investigator in Modern Criminal Investigations" (paper presented at Privacy Issues Forum, Wellington, 27 August 2008); Phil Kitchin "Private Eyes Fight Curbs on Crimebusting" (21 July 2008) *Dominion Post* Wellington 4.

1200 Phil Taylor "The ACC May be Watching You" (8 September 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 19 June 2008).

1201 Nicky Hager "Finding the Enemy Within" (29 May 2007) *Sunday Star-Times* www.stuff.co.nz (accessed 29 May 2007).

1202 Private Security Personnel and Private Investigators Bill 2008, no 297-1, cl 66 (compare to Private Investigators and Security Guards Act 1974, s 52).

1203 Ministry of Justice *Regulating Private Investigators: Review of Private Investigators and Security Guards Act 1974. Discussion Document* (September 2008).

This includes considering whether existing legal restrictions on surveillance by private investigators are appropriate. Pending the outcome of the Law Commission's Review, it is proposed that existing restrictions on visual and audio recording by private investigators will be retained.

Legal controls on surveillance and other intrusions by private investigators

12.46 As the law stands at present, private investigators have no greater legal right to use surveillance or other forms of intrusion than any other member of the public. They are not excluded from the coverage of the Privacy Act, although in some cases they may be able to rely on general exemptions from the information privacy principles. On the other hand, there are currently some surveillance-related restrictions on private investigators that do not apply to other people.

12.47 First, there are restrictions on who may be licensed. The Private Investigators and Security Guards Act provides that there shall be a presumption against licensing or approving private investigators and their responsible employees if they have been convicted of an interception offence under the Crimes Act 1961 (sections 216B-216D) in the previous five years.[1204]

12.48 Secondly, there are restrictions on the use by private investigators of certain types of surveillance device. Section 52 of the Private Investigators and Security Guards Act makes it an offence for a person carrying out the business of a private investigator to take or cause to be taken, or use or accept for use, any photograph, film or video recording of another person, or to record or cause to be recorded a person's voice, without prior written consent.[1205] The origins of this provision lie in Parliament's concern at the time when the Act was passed to protect privacy. The long title of the Act refers to "affording greater protection to the individual's right to privacy against possible invasion by private investigators", and the Act was presented by the Minister of Justice at the time as one of a series of measures planned to deal with different aspects of privacy.[1206] Parliament was particularly concerned about invasions of privacy by private investigators looking for evidence of adultery, and about technological developments that made it possible to photograph or make audio recordings of people covertly from a distance.[1207]

12.49 Although there are restrictions on visual and audio recording by and on behalf of private investigators themselves, there is nothing to prevent them from showing their clients how to install video or audio surveillance equipment. Moreover, a private investigator can also be licensed as a security guard,

1204 Private Investigators and Security Guards Act 1974, ss 17(2)(a), 35(2)(b), and definition of "specified offence" in s 2(1). The Registrar of Private Investigators and Security Guards has discretion to register people with such convictions if, having regard to the nature and circumstances of the offence, the Registrar considers that the application should be granted. Similar provisions are contained in the Private Security Personnel and Private Investigators Bill 2008, no 297-1, cls 17(f)(iii), 41(f)(iii), and definition of "offence of violence" in cl 4. These clauses of the Bill deal with "grounds for disqualification", rather than providing for a presumption against granting applications in certain cases as in the current Act.

1205 There is an exception where a private investigator takes or uses a photograph for the purpose of identifying a person on whom a legal process is being served.

1206 Hon Dr AM Finlay (1 March 1974) 389 NZPD 564-565; (30 July 1974) 392 NZPD 3300-3301.

1207 Hon Dr AM Finlay (1 March 1974) 389 NZPD 565; Mr Wilkinson and Hon Sir Roy Jack (30 July 1974) 392 NZPD 3307, 3316-3317.

and the legislation places no restrictions on surveillance by security guards. Indeed, the Act's definition of "security guard" includes a person who installs, operates or monitors a camera or similar device on premises not owned or occupied by that person "for the purpose of detecting the commission of an offence by any person on those premises".[1208] Thus, it may be that private investigators who are also licensed security guards can install and operate cameras in the latter role. The Registrar of Private Investigators and Security Guards has observed that the line between using surveillance camera footage for the purpose of detecting the commission of an offence and for the purpose of investigating that offence can be quite blurred.[1209]

12.50 There are no specific restrictions on the use by private investigators of other surveillance devices, such as tracking devices, or on the use of visual surveillance devices or listening devices if no recording is made. Nor are there restrictions on the use of covert operatives to monitor people (for example, by watching a house from a parked car), so long as no offences are committed under the general criminal and civil law discussed in chapter 2.

12.51 We do not know for sure how many complaints are received about privacy intrusions by private investigators, whether through the use of surveillance or otherwise, although it appears that there are probably not very many. Between 2003 and 2007, the Privacy Commissioner received eight complaints about private investigators, only one of which was partially upheld.[1210] Complaints can also be made to the Registrar of Private Investigators and Security Guards. The current Registrar reports that he receives few complaints about private investigators, and that complaints about breaches of section 52 are rare.

Issues and reform options

12.52 Private investigators play a legitimate role in providing investigative and other services for the benefit of their clients. In many cases, particularly where the investigation involves allegations of fraud, serious misconduct or criminality, these investigations will also be for the benefit of the wider society. According to Trevor Morley (President of the New Zealand Institute of Professional Investigators), most private investigators in New Zealand carry out investigations into criminal offences, passing on information to the Police once sufficient evidence has been gathered.[1211]

12.53 At the same time, personal information is the stock-in-trade of private investigators, and this information is often obtained by covert means. Part of the job of private investigators is to find out personal information that others wish to keep private. Both the means used to obtain information, and the disclosure of that information, have the potential to intrude significantly on the privacy of the subjects of

1208 Private Investigators and Security Guards Act 1974, s 4(1)(c) and (e).

1209 Phil Taylor "Spying OK in the Eyes of the Law" (5 April 2008) *New Zealand Herald* Auckland B6; see also Joanne Black "Trevor Morley: Private Investigator" (21-27 October 2006) *New Zealand Listener* www.listener.co.nz (accessed 16 October 2006).

1210 Trevor Morley "The Role of the Private Investigator in Modern Criminal Investigations" (paper presented at Privacy Issues Forum, Wellington, 27 August 2008), citing information provided by the Office of the Privacy Commissioner.

1211 Trevor Morley "The Role of the Private Investigator in Modern Criminal Investigations" (paper presented at Privacy Issues Forum, Wellington, 27 August 2008).

investigations. This was an important reason for introducing the licensing of private investigators. As the Minister of Justice at the time put it, the emphasis was on "prevention rather than cure. If we can provide a system of excluding irresponsible people from this occupation we will greatly reduce the risk of abuse."[1212]

12.54 The licensing of private investigators is based, appropriately in our view, on striking a balance between recognising the legitimate role of private investigators and providing protection against possible invasions of privacy. The key question is how this balance should be struck, and, in particular, whether there should continue to be any restrictions on the investigative methods used by private investigators beyond those imposed by the generally-applicable law. We do not propose to explore the option of exempting private investigators from some aspects of the generally-applicable law in relation to privacy and surveillance. We can see no justification for providing such exemptions, and it is our understanding that private investigators are not seeking powers that are greater than those of other members of the public.[1213]

12.55 We have shown in earlier chapters that there are a number of gaps in the existing laws on surveillance and intrusion. Plugging some of these gaps might mean that specific restrictions on surveillance by private investigators are unnecessary, although there could be a case for maintaining the status quo pending wider reform of surveillance laws. We would also be interested to hear whether any current laws relating to privacy, or any of the proposals discussed elsewhere in this issues paper, have particular consequences for the work of private investigators.

Private Investigators and Security Guards Act 1974

12.56 There are two main issues with regard to the Private Investigators and Security Guards Act 1974 (or any legislation that may replace it in future). First, what licensing requirements should be placed on private investigators in order to protect privacy? Secondly, should the Act place any restrictions on the use of surveillance devices by private investigators?

12.57 As we have mentioned, there is currently a presumption against licensing a person who has been convicted in the previous five years of an interception offence under the Crimes Act 1961. These offences are listed, along with various others, as "specified offences" in the Private Investigators and Security Guards Act. There would seem to be a good case for adding other crimes relating to privacy and surveillance to the list of specified offences in the Act, including:

- the intimate covert filming offences;[1214]
- the computer misuse offences;[1215]
- prohibitions on the disclosure of material obtained by lawful surveillance for law enforcement purposes;[1216] and
- any new surveillance legislation that may result from the Law Commission's Review of Privacy.

1212 Hon Dr AM Finlay (1 March 1974) 389 NZPD 565.

1213 Trevor Morley "The Role of the Private Investigator in Modern Criminal Investigations" (paper presented at Privacy Issues Forum, Wellington, 27 August 2008).

1214 Crimes Act 1961, ss 216H-216J.

1215 Crimes Act 1961, ss 249-252.

1216 Crimes Act 1961, s 312K; see also Search and Surveillance Powers Bill 2008, no 300-1, cl 171.

A presumption against licensing people with recent convictions for such offences would help to prevent individuals with records of invading others' privacy from becoming private investigators. There may be other offences that should be added to the list, or other ways in which the licensing process can be used to protect privacy.

12.58 Probably the most controversial provision of the Private Investigators and Security Guards Act is the prohibition on visual and audio recording in section 52. Private investigators objected to this provision when the Act was before Parliament, and they continue to strongly oppose it today.[1217] Section 52 does not appear to have been based on any overseas model, and we are not aware of equivalent legislation in other jurisdictions that contains a similar restriction.

12.59 It was acknowledged when the Act was being considered by Parliament that section 52 could be seen as creating difficulties for private investigators in providing evidence in cases of compensation claim fraud, but the Minister of Justice argued that "in such a case the evidence of a photograph would be quite useless without the supporting statement of the photographer, and if that was available the photograph would be unnecessary."[1218] However, Trevor Morley maintains that section 52 prevents private investigators from obtaining the best possible evidence for their clients in fraud cases:[1219]

> For example, we had an ACC case where a man, who said he could hardly move because of his back injury, was seen lying under this car repairing his gearbox. The best evidence we could produce to the court would be photographs or videotape of people actually doing things contrary to their ACC claims, as opposed to the subjective evidence of the investigator, who may have been observing from a distance.
>
> You then get in a "I said, he said" situation where I say, "He bent over from the waist." "Yes," says his counsel, "but how far did he bend over? Did he really bend over?", and you then get into a huge legal argument which would be very easily resolved by saying, "Hey let's look at the video-tape." But we can't do that. That does grate with a lot of investigators simply because it prevents us doing the very best job for our clients, who in some instances are government departments.

12.60 The question we raise for consideration is whether there is a principled basis for the restrictions in section 52. These restrictions apply only to private investigators and their employees, and not to other people engaging in comparable activity (including private investigators' clients); they apply only to visual and audio surveillance, and not to other forms of surveillance; and they apply only to recording, and not to the use of visual and audio surveillance devices to monitor people without recording them. A more comprehensive legal regime for dealing with surveillance generally might remove the need for specific restrictions

1217 Hon Dr AM Finlay and Mr Wilkinson (30 July 1974) 392 NZPD 3303, 3307; Joanne Black "Trevor Morley: Private Investigator" (21-27 October 2006) *New Zealand Listener* www.listener.co.nz (accessed 16 October 2006); Trevor Morley "The Role of the Private Investigator in Modern Criminal Investigations" (paper presented at Privacy Issues Forum, Wellington, 27 August 2008); Phil Kitchin "Private Eyes Fight Curbs on Crimebusting" (21 July 2008) *Dominion Post* Wellington 4; Regulatory Impact Statement included with Private Security Personnel and Private Investigators Bill 2008, no 297-1 (Explanatory Note) 24, 36.

1218 Hon Dr AM Finlay (30 July 1974) 392 NZPD 3303.

1219 Joanne Black "Trevor Morley: Private Investigator" (21-27 October 2006) *New Zealand Listener* www.listener.co.nz (accessed 16 October 2006).

relating to private investigators. Options for developing such a regime have been put forward in this issues paper. Since the Private Investigators and Security Guards Act was passed, the Privacy Act 1993 has also introduced safeguards in relation to the collection, use and disclosure of personal information, which might apply to video and audio recording by private investigators.

12.61 Specific restrictions on private investigators can only be justified if private investigators are significantly more likely to invade people's privacy, or are likely to invade people's privacy in a more harmful way, than other members of the public. We note that others, such as paparazzi or even ordinary individuals equipped with digital cellphone cameras, are just as capable as private investigators of taking intrusive or embarrassing photographs, or otherwise invading people's privacy.[1220] At the same time, we recognise that there are continuing concerns about the activities of some private investigators. In announcing the proposal to replace the existing Act, the then Associate Justice Minister stated that "A number of high-profile cases over the past few years involving dubious activities by private investigators have, unfortunately, reinforced the need for safeguards."[1221] Such incidents are said to "raise the prospect that significant numbers of private investigators may irresponsibly use the power to photograph and audio-record people without their consent, if given this power."[1222] The Commission would like to hear views on whether such concerns are justified. If they are, it could be that the existing restrictions in section 52 should be extended to cover other forms of surveillance. We emphasise, however, that this issue would need to be considered in relation to any new controls on surveillance applying to the public generally that may be introduced as a result of the Commission's Review.

Other mechanisms

12.62 There are other options for regulating privacy-intrusive activities by private investigators, such as surveillance, if it is considered that additional regulation is needed. The Private Investigators and Security Guards Act provides for the making of regulations prescribing codes of ethics for private investigators and their responsible employees, and contravention of such codes constitutes misconduct.[1223] Misconduct is grounds for a complaint against an investigator, and can result in the investigator's licence being suspended or cancelled, among

1220 In this regard, it is important to note the list of activities that are excluded from the requirement to register as a private investigator, including seeking, obtaining or supplying information for purposes relating to the dissemination of news or other information to the public: Private Investigators and Security Guards Act 1974, s 3(4).

1221 Clayton Cosgrove, Associate Minister of Justice (Speech to the New Zealand Security Conference, Auckland, 25 June 2008). For examples of alleged "dubious activities" by private investigators see Audrey Young "Brethren Spy Hits Back at Labour" (23 September 2006) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 30 October 2008); David Fisher "Brethren Spy Comes in from the Cold" (1 October 2006) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 30 October 2008); Nicky Hager "Finding the Enemy Within" (29 May 2007) *Sunday Star-Times* www.stuff.co.nz (accessed 29 May 2007).

1222 Regulatory Impact Statement included with Private Security Personnel and Private Investigators Bill 2008, no 297-1 (Explanatory Note) 31.

1223 Private Investigators and Security Guards Act 1974, s 71(h).

other penalties.[1224] No codes of ethics have ever been made under the Act, but a code or codes could be developed to regulate surveillance or other activities of private investigators that may breach the privacy of individuals.

12.63 A second option would be for the Privacy Commissioner to develop a code of practice under Part 6 of the Privacy Act 1993, prescribing how the information privacy principles apply to the private investigation industry. Alternatively, or in addition, the Privacy Commissioner could produce guidance notes on the application of the Privacy Act for private investigators.

12.64 Finally, there is the option of industry self-regulation. The New Zealand Institute of Professional Investigators Inc (NZIPI) is a professional body representing over 100 private investigators.[1225] It has a code of ethics, but it is very brief, and does not specifically mention privacy. Alleged breaches of the code are investigated by an Ethics Committee, which makes recommendations to the Executive of the Institute about what action, if any, should be taken. The NZIPI or another suitable industry body could develop a more detailed code of ethics, incorporating protection of privacy. The drawbacks of this approach are that it would apply only to those private investigators who are members of the professional organisation, and would carry no legal sanctions.

Q80 Should private investigators be subject to any greater legal restrictions than other members of the public in order to protect privacy?

Q81 Do any of the current laws relating to privacy, or any proposals for possible law reform, discussed elsewhere in this issues paper have particular implications for private investigators?

Q82 Should additional privacy-related crimes be added to the list of "specified offences" in the Private Investigators and Security Guards Act 1974? Are there any other ways in which the licensing process could be used to protect privacy?

Q83 Should section 52 of the Private Investigators and Security Guards Act 1974 be retained? If so, should it be modified in any way?

Q84 Should surveillance and other privacy-intrusive activities by private investigators be regulated by any of the following: a code of ethics made under the Private Investigators and Security Guards Act 1974; a Code of Practice made under the Privacy Act 1993; or a code of ethics developed and enforced by the industry itself?

1224 Private Investigators and Security Guards Act 1974, ss 53, 57-58.

1225 See the website www.nzipi.org.nz.

Part 4
OVERVIEW

Chapter 13
Overview

13.1 Privacy is an important social value. It is also increasingly becoming an issue for the law. As the potential modes of invasion of privacy increase with the development of modern technology, it is necessary for us to examine whether the legal protections are sufficient. This exercise is an important but complex one. In this chapter we attempt to sum up the problems faced, and the issues raised, in this issues paper.

SOME DIFFICULTIES

Problems of definition

13.2 The difficulty of defining privacy is well-known. The lack of clear boundaries of the very subject matter has rendered our task a particularly difficult one.

13.3 Privacy and other interests are mixed together in some parts of the law. On the one hand, in the case of a number of rules which are privacy-related it is clear that interests in addition to privacy are protected by them, and that other policies underlie them. Thus, the rules allowing a court to be cleared in certain types of proceedings often protect the privacy of those involved, but also advance the important interest in the administration of justice. On the other hand, some rules of law which are primarily directed to other interests may tangentially protect privacy as well. We have noted that a number of specific torts, such for example as trespass and defamation, may occasionally protect privacy. Likewise, the rules about secrecy of tax details, while mostly directed to the integrity of the tax system, are seen by many as privacy-related. This mix of policies and interests means that we must think carefully before making significant amendments to these rules. It is all too easy to over-simplify what is at stake.

13.4 The definitional difficulty also means that some privacy rules are expressed in such broad terms that their boundaries are unclear. The *Hosking* tort is perhaps the best example, requiring as it does "facts in respect of which there is a reasonable expectation of privacy". The danger of rules as wide as this is that, unless carefully controlled, privacy may overflow its boundaries and spread into matters which are merely ones of good taste, or which properly belong to the realm of secrecy rather than privacy. In other words, privacy protection may end up protecting more than was initially intended.

13.5 For these reasons we had often, in the course of this project, to consider whether certain matters were within its scope: matters such as court suppression orders, powers of entry to property, or the obtaining of information by deceptive practice.

The difficulty of drawing lines

13.6 Perhaps because of this indeterminacy it has been difficult to draw various aspects of privacy with bright lines. So, for example:

- We have found the distinction between spatial and informational privacy to be a useful one, but acknowledge that it is not a perfect division. There are areas of overlap. Intrusions into spatial privacy are often made with the purpose of acquiring information and later publishing it. Moreover, certain activity which is clearly an invasion of privacy does not fit comfortably under either heading; improper access to a computer may be an example. Despite these overlaps, we have nevertheless found the distinction a useful one and have used it in this paper, acknowledging the difficulties when they arise.
- Likewise, the line between surveillance and other forms of intrusion is not a sharp one. For purposes of exposition we have assumed in this paper that surveillance involves the use of devices to monitor people. This, in a few cases, has led to the drawing of artificial distinctions. Again, however, we have found the categorisation helpful for purposes of exposition.
- There is another distinction of a different kind. A good part of this issues paper is about the enforcement of privacy in the courts. However, it soon became evident to us that we needed to ask whether the complaints provisions of the Privacy Act adequately cover some aspects. It would be unproductive, and is sometimes simply not possible, to look at the various forms of enforcement in isolation. So to do would be to fail to see the whole picture.

The size of the project

13.7 Privacy is a very large topic. It has many facets, and intrusions into it can take many forms. This has at least three consequences. First, the subject-matter deals with a range of very unlike types of conduct, and also types of conduct which are alike but which have differing levels of impact. Some breaches of privacy create significant financial risk. Others could conceivably cause risks to health and safety. Even those many intrusions which impact on feelings and human dignity can do so with varying levels of severity: intimate covert filming has a much greater effect on the subject than, for example, intrusion by telemarketing. For this reason we must be very careful not to resort to simplistic generalised solutions. One size does not necessarily fit all. Workplace privacy, for instance, has many different features from the privacy of the home. Rules must be tailored to suit the specific type of invasion of privacy which is in issue. The consequence

may be that the certainty and coherence which are so desirable in many branches of the law are not readily achievable in privacy. Indeed, in this field of study they may sometimes lead to injustice.

13.8 A second consequence of the size of the topic is that we have had to exclude certain aspects simply because to pursue them would have made the project unwieldy. Thus, we have decided not to deal in this project with the many statutes and other rules of law conferring on various persons and agencies powers of entry to property. We note that our report on *Search and Surveillance Powers* already deals with some of these powers.

13.9 A third consequence is that there may be aspects of the topic that we have overlooked. We make no claim to total coverage or completeness. It is for this reason that we ask the question of submitters as to whether there are any matters which they feel should have been covered but which are not.

Strength of opinions

13.10 Privacy is a field which induces strong feelings in people. On some matters opinion is polarised. That is evident even in the judgments in *Hosking v Runting*, where three judges believed there should be a tort of invasion of privacy, whereas the other two dissented very strongly indeed. There are some who would strengthen the Privacy Act and enhance the powers of the Privacy Commissioner, while others believe the Act currently goes too far and should be reduced in coverage and scope. Some of these views may be misguided, but they do exist. The Commission expects therefore that submissions on this issues paper will differ widely.

Relationship to other projects

13.11 The Commission's privacy project is divided into four stages. The first resulted in the publication of a study paper, *Privacy: Concepts and Issues*. The second led to a report on *Public Registers*. This, the third stage, has drawn upon the conclusions arrived at in Stage 1, and inevitably has connections with, and implications for, Stage 4: a review of the Privacy Act 1993, which is already under way. We have noted that it has not been possible or sensible to divide off remedies and sanctions available under the Privacy Act from those available from other courts and tribunals. It is important to see the range of remedies as a whole. So some of the issues we have identified in this paper will be relevant also at Stage 4. The final reports on Stages 3 and 4 will be closely related.

13.12 Finally, we would note that this issues paper should also be seen in the context of the Law Commission's report on *Search and Surveillance Powers*. A Bill to implement that report is before Parliament at the time of writing. That Bill is concerned with the surveillance and search powers of law enforcement agencies. It contains provisions about the need for warrants, and the limits on enforcement agencies' powers to keep persons and property under surveillance. It would be anomalous indeed if law enforcement agencies were under constraints, but private individuals were not. In this issues paper we seek to find solutions to the question of how far private individuals, and agencies other than law enforcement agencies, should be controlled by the law when engaged in surveillance-type activities.

THE PRESENT LAW

13.13 There is little shape or coherence about the present legal protections of privacy. The landscape contains the following features.

13.14 First, as we have seen, there is a mixture of types of enforcement. There is some criminal law. Much of it is concerned with intrusion, and the safeguarding of information obtained in confidence. Even then the coverage is far from complete. The *Hosking* tort, on the other hand, provides for civil action, but to date it only covers the disclosure of information and not the various forms of intrusive conduct. The Privacy Act is mainly about the collection, security and use of personal information, and is enforceable by a complaints process. Complaints against the media can be dealt with by the Broadcasting Standards Authority and the Press Council. This immediately raises questions as to which mode of enforcement is best suited to particular types of breach. Is there a good reason why the criminal law provides no sanctions for disclosure of personal information per se (as opposed to penalties for disclosure that are based on the manner in which the information was obtained), while the *Hosking* tort provides a remedy for nothing else? Not much attention has ever been paid to questions of this kind. Sometimes a person whose privacy is infringed may be able to proceed under more than one mode.

13.15 Secondly, the rules are a mix of general and specific. Some of the criminal offences are so specific that they cover only a small part of the field and leave gaps. However, the tort, and the broadcasting legislation, could scarcely be framed in more general terms.

13.16 Thirdly, as we have indicated, the coverage of the law is strangely incomplete. In particular, surveillance is most incompletely dealt with. That may seem strange, because it is probably the form of invasion which frightens people most. Its inadequacy is in part due to the fact that the law has simply not kept pace with advances in technology. In this the law of privacy is not alone. The internet and other forms of new technology are posing challenges for the law in many areas.

13.17 Fourthly, there is much uncertainty in the present law. The scope of the *Hosking* tort, as we have shown, is far from well defined. The application of the Privacy Act to various types of surveillance is also open to argument. The Broadcasting Standards Authority has had to construct its own principles because the Broadcasting Act 1989 leaves the matter so much at large. While some uncertainty is inevitable, excessive uncertainty has untoward effects. It can constrain conduct more than is reasonable or justifiable. It can also involve costs.

13.18 Fifthly, there are inconsistencies in the law. That is particularly evident in the area of criminal penalties, and in the ingredients of, and defences to, the several criminal offences.

13.19 In the course of this issues paper we have attempted to expose areas where the coverage of the law is inadequate or problematic for any of the above reasons. We ask for submissions as to how these problems can best be resolved.

REFORM OF THE LAW

13.20 When considering reform there are a number of fundamental questions.

Types of enforcement

13.21 The first question is what type of enforcement is most suitable to the particular situation.

- *Criminal law* – In chapter 5 we considered some criteria for when criminal liability is appropriate. It should be reserved for serious cases, where the interests of the public are involved. There may be some instances where existing offences are not justified, but great care is needed before any decision is made to repeal any of them. All aspects of their underlying policies need to be examined. Careful consideration will also be needed as to whether further offences should be created.
- *Civil action in the courts* – Civil action in the courts is expensive, generally slow, and subject to what at times can be complex procedural rules. Consideration needs to be given to whether it is the best way of providing for individual persons to obtain redress for intangible injury. It may be that in the field of privacy access to a complaints procedure or a tribunal which can deliver cheap and speedy solutions is a better way forward. It is the way in which most other injuries to dignity are currently redressed; for example, the discrimination provisions of the human rights legislation. It remains true, however, that there are things which a court can do which no other agency can, and the grant of injunctions is one of them. As we have shown, careful consideration should be given to when tort actions are, and are not, appropriate. It may be possible to make explicit statutory provision for civil remedies for the breach of some statutory duties.
- *Lower-level enforcement* – If it is decided that certain types of breach of privacy are best redressed by agencies outside the court system, the question then arises as to which of those agencies is the most suitable. In what cases can the Privacy Act be relied on to provide all the redress that is necessary? Would it be advantageous to extend or modify the provisions of that Act so that it covers things which it currently does not? In what cases might there be advantage in a separate body or tribunal? (We note that currently the media are dealt with by their own tribunals).
- *Other types of regulation* – In some overseas jurisdictions there have been proposals for other forms of regulation. Just as law enforcement officers need a warrant to engage in certain types of surveillance, could there even be an argument that surveillance carried out by other persons should need a specific licence or authority? One assumes that regimes of this kind would be exceptional, and would only be introduced after careful analysis of the respective costs and benefits. It would also need to be considered how such regimes would be enforced, and by whom.
- *Codes of practice* – It may be that in some instances codes of practice specific to a particular industry or activity may be the most satisfactory response. The question then arises of how those codes are to be enforced. The Privacy Commissioner currently has the power to make codes for particular industries: they then become enforceable by complaint under the Act in the ordinary way. Likewise, the Broadcasting Standards Authority has formulated codes for the various types of broadcasters; they, too, are enforced by a complaints

process. There may even sometimes be room for non-binding codes which stand outside the law and have the effect of guidelines. Self-regulation is sometimes a useful beginning.

13.22 Careful judgment is required in making these choices. One does not necessarily have to conclude that only one form of enforcement is appropriate to each type of privacy invasion, although this will often be the case. Alternative sanctions are far from unknown in our law. Indeed, under the law as it presently stands it is conceivable that the subject matter of a complaint to the Broadcasting Standards Authority might also involve a trespass which could be sued on in court as a tort, or even prosecuted under the provisions of the Trespass Act 1980. There can eventually come a point, however, when a plethora of alternative remedies can lead to confusion, particularly if the exact criteria for the different types of enforcement are inconsistent with one another. We should aim for as much simplicity and clarity as possible.

Types of rules

13.23 There is also a question as to how specific or how general the formulation of rules should be. Generally speaking, rules of the criminal law are expressed in more detailed and specific particularity than are the principles of the civil law. It may be that where it is a tribunal rather than the court which enforces the law, some generality of expression which allows scope for discretion may be desirable.

13.24 Each of the types of rule has its particular advantages and disadvantages. Let us first consider rules which are broad and general. The broader the reach of the rule, the more uncertain its application, and the greater the danger that too much will be covered by it. Generality can also lead enforcers to fail to draw necessary distinctions between types of conduct which really are different. We have noted in our discussion of surveillance that it may be preferable to have specific rules for devices with different functions (visual, interception, tracking, and so on) rather than to attempt in general language to cover all types of surveillance. Necessary differences are too readily lost in vague language. Broad rules also lead to uncertainty; and people who are uncertain as to what their liabilities are often unnecessarily constrain their conduct. Rules which constrain freedom of expression because of their uncertainty are to be avoided where possible. Just as uncertainty can be inhibiting, so can it be costly. People subject to the law may need to take legal advice.

13.25 Yet detailed rules have their drawbacks too. If rules are too detailed one can become lost in a wilderness of single instances, and principle can too readily be lost. Moreover, detail can leave gaps, particularly in the face of new developments in society and technology. Specific provisions do not move with the times as effectively as those cast in more general language.

13.26 The balance to be drawn between detailed and general principles is an eternal problem for law makers. It is particularly acute in the area of privacy.

Statute or common law

13.27 Inevitably, most of our privacy law is statutory. All criminal law has to be, as does law which is enforced by an agency, because the latter's powers can only be conferred by statute. There are, however, a few areas of privacy protection which are common law. We have confronted the question of whether some of them should be codified, so that the whole field of privacy protection is statutory. When dealing with the *Hosking* tort we canvassed the pros and the cons of this question. A particular issue for this project is that if it were to be decided to introduce a tort of intrusion it would have to be done by statute for the simple reason that no common law on the topic exists. The question would then arise whether it would be sensible to have a statutory intrusion tort standing alongside the *Hosking* publicity tort which remained common law.

CONTEXT AND BALANCE

13.28 It has been a recurring theme of both this issues paper and our study paper *Privacy: Concepts and Issues* that protection of privacy involves a balancing process.

Public interest

13.29 The interest in privacy must always be weighed against other public interests. Privacy is seldom an absolute value. Public interest can appear in various forms in the rules which protect privacy. Sometimes it is an overriding defence, as in the *Hosking* tort and the BSA privacy principles. The question whether in a particular case the matter is one of public concern or public interest must be determined by the judge or tribunal. Yet in other contexts the relevant rule of law, rather than providing generally for a public interest defence, lists quite specific exceptions. The Privacy Act is the best example. Its broad privacy principles are in each instance subject to a list of specific exceptions relating to such matters as health, public safety, law enforcement, and so on. In other words that Act, rather than relying on a broadly-stated public interest exception, has preferred to itemise particular instances of public interest. Which of these methods is the best? The question can be particularly acute in the field of criminal law, where certainty is important. Broad defences such as "public interest" or "reasonable excuse" do not conduce to certainty, but sometimes do allow the actor some scope for sensible judgement.

13.30 A related question is how far the media should be special. Our fourth estate performs an essential role in a democratic society, and it may be argued that it deserves special recognition, and should be specially exempted from certain of the rules. That indeed has happened in the Privacy Act: the media are exempt as long as they are engaging in news activities. However, the increasing difficulty of defining the term "media" in the digital age, and the undoubted truth that freedom of speech is a privilege of everyone, and not just the media, may make the special defence argument less sustainable in certain contexts.

Bill of Rights Act

13.31 The relationship of privacy to the rights and freedoms in the New Zealand Bill of Rights Act 1990 has been a matter of wide discussion and controversy. Unlike the position in some other jurisdictions, privacy is not explicitly protected in our Bill of Rights, although an argument is occasionally made that it is

preserved by the savings provision in the Act. Whichever view is taken of this, the question again comes down to one of balancing. In all cases, privacy must be weighed against the other rights and freedoms in the Act, the question being whether privacy is a justified limitation on those other rights and freedoms. The right with which it most usually comes into contest is freedom of information. It is not yet entirely clear whether the omission of privacy from the express provisions of the Bill of Rights Act will make a difference by comparison with the United Kingdom approach where privacy finds an express place in the European Convention on Human Rights.

Compliance costs

13.32 In formulating any privacy regime, the desirability of protecting privacy must be weighed against the compliance costs which will be involved. The protection of privacy is sometimes not a cheap matter. It may involve the setting up of systems, and the employment of additional staff. In this regard uncertain law brings its own costs as intimated above. If the law is not clear, legal advice may be required and even then that legal advice may be able to do no more than assess the risks of certain conduct without giving a firm answer.

13.33 Nor is it only those subject to the privacy laws on whom the costs may fall. Enforcement can also be a costly business. Indeed, law which is uncertain or complex, or disproportionately severe, may be so expensive to enforce that it ends up not being enforced at all.

13.34 When formulating rules to protect privacy, it is important that cost-benefit analyses be undertaken. Those laws should not go further than reasonably necessary to protect the interests at stake. No one wants a costly or unwieldy bureaucracy.

LESSONS FROM OTHER JURISDICTIONS

13.35 In this paper we have looked at the privacy protection provided by legal systems of other jurisdictions, in particular Australia, Canada, the United Kingdom, Ireland, Europe and the United States. We noted that in many of them there is to be found the same untidy mix of civil and criminal law and regulatory regimes. New Zealand does not stand alone in the untidiness and incompleteness of its current protection. This does not mean that we do not need to try to do better. But three points should be made.

13.36 First, we must be careful not to borrow unthinkingly from other jurisdictions. It is important to do what is best here, given our own society, our own media culture and our own subjection to international influences. Even if we conclude that the New Zealand context is very similar to that in other countries, that is no reason for assuming that we should copy blindly, rather than trying to fashion our own solutions.

13.37 Secondly, we should note that in some overseas jurisdictions certain aspects of privacy law have proved less than effective. The Canadian statutory torts have been very seldom used, and even more seldom have resulted in plaintiff victory. The equivalent of the *Hosking* tort in the United States very seldom favours a plaintiff in the face of the media.

13.38 Thirdly, we may note the influence abroad of the polarisation of opinion which we noted earlier to be a feature of privacy law. A number of attempts in other jurisdictions to introduce statutory torts of various kinds, and to implement comprehensive surveillance control regimes, have met with strong opposition from various sectors of the community. This has sometimes resulted in failure to implement them. We are conscious of the need to listen to the concerns of all sectors, and to propose reforms which achieve a sensible and reasonable balance.

CONCLUSION

13.39 In this paper we have dealt with a wide range of subject matter, and have looked at a range of options for dealing with the problems which our research has revealed. The Commission is currently committed to no particular model or set of options. A number of approaches are possible. We seek input from as wide a range of people and points of view as possible.

Q85 Are there any other matters relating to the adequacy of New Zealand law to protect privacy that have not been covered in this issues paper, and that you believe the Commission should consider? (Note that the Privacy Act 1993 is to be the subject of a separate issues paper.)

Appendix

Appendix

List of questions

The Commission welcomes your views on the following questions. Feel free to answer as many or as few questions as you like. You should also feel free to make any other comments or submissions in relation to the issues raised in this issues paper. Information on how to make a submission appears at the start of the paper.

CHAPTER 7

Q1 Is there value in a tort of invasion of privacy by publicity given to private facts? If so, what is that value?

Q2 Do you think it would be sensible to abolish the tort without replacing it? If it is to be replaced, what should replace it?

Q3 If there is to be a tort, is it better to codify it in statute, or leave it to evolve by case law?

Q4 If there is to be a statute, what should it contain? It would be helpful if you answered the specific questions 5-23 below, but you need not confine yourself to those questions.

Q5 Should the "highly offensive" test remain as a separate element of the tort?

Q6 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?

Q7 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?

Q8 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?

Q9 In what circumstances can there be a reasonable expectation of privacy in relation to something which has already been published?

Q10 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?

Q11 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?

Q12 Would it be helpful, in a statute, to give examples of matters which are normally of legitimate public concern?

Q13 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?

Q14 Other than legitimate "public concern", what defences should there be to a cause of action for publicity given to private facts?

Q15 What remedies should be available?

Q16 Is it possible, or desirable, to list considerations to be taken into account in assessing damages?

Q17 Should it be possible to obtain a remedy in this privacy tort (or cause of action) if some or all the statements made about the plaintiff are untrue?

Q18 Should wide publicity be required to ground a cause of action or might publication to a small group be enough in some cases?

Q19 Should it ever be possible to obtain a remedy for invasion of the privacy of a deceased person?

Q20 Should corporations, or other artificial persons, be able to bring an action for invasion of privacy?

Q21 Is it possible to lay down a statutory test to clarify the special position of children?

Q22 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?

Q23 What mental element should be required to found liability in a defendant?

Q24 Should the existing criminal offences relating to disclosure of personal information be examined to see whether they are all still needed? Are there any existing offences that are no longer needed?

Q25 Are any new criminal offences needed?

Q26 Is it worthy of consideration whether the Privacy Act 1993 should contain offences?

Q27 Should inconsistencies in the existing criminal offences and penalties be removed? If so, how?

Q28 Are any other civil remedies in relation to disclosure of personal information needed? If so, should they be obtainable in the courts, or in some other forum?

CHAPTER 8

Q29 How useful are the distinctions between public and private places, mass and targeted surveillance, and overt and covert surveillance, for the purpose of framing laws to control surveillance? Are there any other key distinctions the Commission should consider?

Q30 Are there particular surveillance technologies that you are especially concerned about?

Q31 What role do you see for privacy-enhancing technologies in addressing the problems of surveillance? Is there a role for the law in promoting or mandating such technologies?

Q32 Which of the following types of surveillance are you particularly concerned about? What are your main concerns about these types of surveillance? Which of these types of surveillance do you consider particularly beneficial, and why? (Note that surveillance for intelligence and law enforcement purposes is largely outside the scope of this Review, and that workplace, private investigator and media surveillance are discussed in chapter 12.)

- Regulatory (including local government, environmental and traffic regulation)
- Security (including CCTV)
- Commercial
- Domestic
- Research
- Workplace
- Private Investigator
- Media
- Other

CHAPTER 10

Q33 Should civil liability for certain uses of surveillance devices be provided for by means of a statutory privacy tort or intrusion tort (as discussed in chapter 11), or a statutory surveillance tort? If so, what uses of surveillance devices should the tort cover?

Q34 Should civil liability for the use of surveillance devices be based on breach of a statutory duty?

Q35 Should certain targeted surveillance activities be designated "specified acts" of harassment under the Harassment Act?

Q36 Should certain acts of surveillance be considered to constitute harassment on their own, without a requirement for any further specified act directed at the applicant to occur, for the purposes of seeking a restraining order or bringing a criminal charge under the Harassment Act 1997?

Q37 Should the use of surveillance devices continue to be dealt with under the criminal law by targeting specific uses of surveillance devices in particular circumstances? Alternatively, should these offences be dealt with more generically? If so, how could this be achieved?

Q38 Are any reforms to the criminal law relating to visual surveillance required, such as:

- a new visual surveillance device offence;
- reform of the summary offence for offensive behaviour in a public place or a new offence to cover intrusive visual surveillance in public;
- an offence against the use of hidden cameras; or
- expansion of the intimate visual recording offence?

Q39 Should any of these matters concerning visual surveillance be dealt with instead by way of civil liability (under a tort or the Privacy Act)?

Q40 What should be the scope of any new visual surveillance offences?

Q41 Does the definition of "private communication" for the purposes of the interception offence require reform?

Q42 Should the participant monitoring exception to the interception offence be reformed in any respect?

Q43 Are any other reforms of the interception offence required?

Q44 Are any other reforms required in relation to communications privacy?

Q45 Should a new offence be created to target the covert use of tracking devices to determine people's locations?

Q46 Are the computer misuse offences adequate to deal with privacy intrusions from computer hacking and other unauthorised access to computers and digital devices, and the use of spyware and keystroke loggers? Is a specific review of the adequacy of these offences required?

Q47 Should consideration be given to an offence for the unauthorised monitoring or collection of call data? Or should this be dealt with as a matter of civil liability?

Q48 Should consideration be given to an offence against RFID skimming in New Zealand?

Q49 Should the application of the Privacy Act to surveillance be clarified? If so, how should this be done?

Q50 Do the privacy principles need any modification in the way they apply to surveillance? If so, how should they be modified?

Q51 Is a new set of surveillance principles required, either within the Privacy Act framework or under a new Surveillance Act? If so, what should be the content of these principles, and how should they operate?

Q52 Should there be limitations on surveillance of public spaces carried out by both public and non-public agencies?

Q53 Should CCTV be regulated under a specific CCTV statute?

Q54 If not, should CCTV be regulated in any other way such as:

- the Local Government Act;
- statutory regulations;
- a Code of Practice issued by the Privacy Commissioner;
- voluntary guidelines issued by the Privacy Commissioner; or
- standards developed by Standards New Zealand?

Q55 What are the most important issues that any regulation of CCTV should cover?

Q56 Are any specific regulatory measures needed in relation to RFID technology?

Q57 Are any other regulatory measures necessary or desirable in relation to surveillance?

CHAPTER 11

Q58 Should the Harassment Act 1997 provide for the award of damages?

Q59 Are any reforms to the law needed to deal with voyeurism not involving the use of recording devices, including reform of the "peeping and peering" offence in the Summary Offences Act 1981?

Q60 Are any new criminal offences, or changes to existing offences, needed to deal with specific types of intrusion other than surveillance?

Q61 Are any new civil remedies (apart from a possible intrusion tort) needed to deal with intrusion?

Q62 Should an express right to sue for breach of statutory duty be created in relation to any statutory provisions relating to intrusion?

Q63 Should there be an intrusion tort?

Q64 Should the development of an intrusion tort be left to the common law, or should it be introduced by statute?

Q65 If an intrusion tort is to be introduced by statute, what should be its elements? Specifically:

- Should it refer to intrusions on "solitude and seclusion", and would this necessarily suggest that it applies only in private places?
- Should it include intrusions into personal or private affairs and concerns, or should it be limited to intrusions into spatial privacy (unwanted access to our persons and private spaces)?
- Should it include examples?

Q66 Would your answers to questions 5-8 and 11 from chapter 7 differ for the intrusion tort from the answers you gave with respect to the disclosure tort?

Q67 If the statute were to give examples of matters of public concern, would the examples for the intrusion tort differ in any respects from those for the disclosure tort?

Q68 With respect to the intrusion tort, should the statute require only reasonable grounds for belief that the intrusion was for the purpose of obtaining information in the public interest or about matters of legitimate public concern, or should the test be an objective one?

Q69 Would your answers to questions 14-16, 19-21 and 23 from chapter 7 differ for the intrusion tort from the answers you gave with respect to the disclosure tort?

Q70 What do you think should be the relationship between the disclosure and intrusion torts if both were to be put on a statutory basis?

Q71 Should there be a mechanism for dealing with intrusion at a lower level as an alternative to proceeding through the courts? If so, what form should this take? Should intrusion and disclosure both be dealt with at the same level?

CHAPTER 12

Q72 Should the media be subject to any greater, or lesser, legal restrictions concerning surveillance and other intrusions than other members of the public?

Q73 Does the current framework of content regulation by the BSA and the Press Council provide adequate protection against intrusions by the media? Alternatively, does it go too far in limiting media freedom?

Q74 To what extent should the media be exempted from laws dealing with surveillance and other intrusions (either current laws, or options for reform discussed in this issues paper)?

Q75 What form should any exemptions for the media take? Should they be restricted to newsgathering, and if so, how should newsgathering be distinguished from entertainment?

Q76 Are the issues relating to surveillance and other forms of intrusion in employment significantly different from issues in other areas? If so, how?

Q77 Does the current legal framework achieve an appropriate balance between the interests of employers and employees with regard to surveillance and other forms of intrusion? If not, in what areas is reform needed to achieve an appropriate balance?

Q78 Should there be a specific statute governing workplace surveillance? If so, what areas should it cover?

Q79 Should there be a code governing workplace surveillance or workplace privacy generally? If so, what areas should it cover, and what mechanism should be used to introduce it?

Q80 Should private investigators be subject to any greater legal restrictions than other members of the public in order to protect privacy?

Q81 Do any of the current laws relating to privacy, or any proposals for possible law reform, discussed elsewhere in this issues paper have particular implications for private investigators?

Q82 Should additional privacy-related crimes be added to the list of "specified offences" in the Private Investigators and Security Guards Act 1974? Are there any other ways in which the licensing process could be used to protect privacy?

Q83 Should section 52 of the Private Investigators and Security Guards Act 1974 be retained? If so, should it be modified in any way?

Q84 Should surveillance and other privacy-intrusive activities by private investigators be regulated by any of the following: a code of ethics made under the Private Investigators and Security Guards Act 1974; a Code of Practice made under the Privacy Act 1993; or a code of ethics developed and enforced by the industry itself?

CHAPTER 13

Q85 Are there any other matters relating to the adequacy of New Zealand law to protect privacy that have not been covered in this issues paper, and that you believe the Commission should consider? (Note that the Privacy Act 1993 is to be the subject of a separate issues paper.)

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.