LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

January 2008, Wellington, New Zealand | STUDY PAPER 19

PRIVACY
CONCEPTS AND ISSUES

REVIEW OF THE LAW OF PRIVACY
STAGE 1

LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

January 2008, Wellington, New Zealand | STUDY PAPER 19

PRIVACY: CONCEPTS AND ISSUES

REVIEW OF THE LAW OF PRIVACY STAGE 1

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 – President

Dr Warren Young – Deputy President

Helen Aikman QC

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 6001, New Zealand

Document Exchange Number: sp 23534

Telephone: (04) 473-3453, Facsimile: (04) 914-4760

Email: com@lawcom.govt.nz

Internet: www.lawcom.govt.nz

National Library of New Zealand Cataloguing-in-Publication Data

Privacy : concepts and issues : review of the law of privacy : stage 1.

(New Zealand Law Commission study paper ; 19)

ISBN 978-1-877316-43-2

1. Privacy, Right of—New Zealand. I. New Zealand.

Law Commission. II. Series: Study paper (New Zealand.

Law Commission) ; 19.

342.930858—dc 22

Study Paper/Law Commission, Wellington, 2008

ISSN 1174-9776 (Print)

ISSN 1177-7125 (Online)

ISBN 978-1-877316-43-2

This report may be cited as: NZLC SP19

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

Privacy: Concepts and Issues

Review of the Law of Privacy Stage 1

CONTENTS

CHAPTER 2

CHAPTER 3

CHAPTER 4

FOREWORD

For centuries the term privacy was hardly known to the law. In the late 20th century it burgeoned into a fully-fledged notion that took on many different characteristics. No one doubts that privacy is important, but there is much that is elusive and uncertain about the concept. In this first stage of the Privacy Review being conducted by the Law Commission, we concentrate on the conceptual and theoretical questions that arise in the field of privacy. We make a hard-headed analytical effort to get to grips with what it means and how it may be approached as a matter of policy. We also identify some of the developments that have an impact on privacy, and some issues for further exploration in later stages of this Review.

This study paper contains no policy recommendations: these will be left to the later stages of the Review. Stage 2 relates to public registers, stage 3 will consider the adequacy of New Zealand civil and criminal law to deal with invasions of privacy, and stage 4 will comprise a review of the Privacy Act 1993.

Modern technology has changed our lives and, more than any other development, technological change has raised the salience of the privacy issue. In this paper we look at developments in technology, as well as international developments. We examine the theoretical and conceptual issues surrounding the concept of privacy, and discuss what the appropriate policy approach is. We look at social attitudes to privacy and the state of public opinion. We consider the emerging practices of surveillance. In the last chapter we discuss some issues that we think are important, and that will need more attention in subsequent stages of this privacy Review.

A lot of research has gone into this project and it has been demanding on the Law Commission's Legal and Policy Advisers. This study paper has been peer reviewed. We wish to thank Nicole Moreham of Victoria University of Wellington and Charles Raab of the University of Edinburgh for carrying out these peer reviews. The study paper was refined considerably as a result. We wish to acknowledge our debt to the Privacy Commissioner Marie Shroff and her staff, with whom we have had regular meetings. They have helped us to become familiar with the working of privacy law at the coalface. They will not agree with everything here, but their help to us has been substantial.

This project was worked on by Joanna Hayward, Mark Hickford and Ewan Morris. Rachel Hayward and Janet November, who worked on stage 2 of this Review, also assisted with this study paper. The Commissioners responsible for the project were Geoffrey Palmer and John Burrows.

Geoffrey Palmer
President

TERMS OF REFERENCE

Review of privacy values, technology change, and international trends, and their implications for New Zealand law

This project will proceed in stages, with reports made at each stage.

In stage 1 of the project, the Law Commission will undertake a high level policy overview to assess privacy values, changes in technology, international trends, and their implications for New Zealand civil, criminal and statute law. The Law Commission will conduct a survey of these trends in conjunction with the Australian Law Reform Commission. A report on this overview will be published.

In stage 2 of the project, the Law Commission will consider whether the law relating to public registers requires systematic alteration as a result of privacy considerations and emerging technology.

In stage 3 of the project, the Commission will consider and report on:

(a) The adequacy of New Zealand's civil law 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.

In stage 4 of the project, the Commission will review the Privacy Act 1993 with a view to updating it, taking into account any changes in the legislation that have been made by the time this stage of the project is reached.

Summary

THE LAW COMMISSION'S REVIEW OF PRIVACY

1 The Law Commission is conducting a Review of Privacy ("the Review") in four stages, of which this study paper is the first stage. Later stages will examine the law relating to public registers; the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy; and the Privacy Act 1993 itself. The aims of this study paper are to provide a conceptual framework for the Review; to review social, technological and international developments that may have an impact on privacy in New Zealand; and to identify some key issues and implications for law and policy that will be considered in more depth in later stages of the Review.

ISSUES OF THEORY

2 This study paper begins with an analysis of privacy from a conceptual point of view. As discussed in chapters 2 and 3 of this study paper, privacy is an elastic, complex and multi-faceted concept that is notoriously difficult to define. There are many competing theories and definitions of privacy. Indeed, some commentators have expressed the view that privacy is an unsatisfactory term in that it has "a protean capacity to be all things to all lawyers", or that it is so vague and elastic as to defy definition.

3 However, the Law Commission, in conducting this Review, has taken the view that it is very important to try to find out what privacy means. While definitive conclusions may be difficult to reach, this study paper sets out to offer a conceptual framework for analysing claims about privacy. To this end, we have engaged in a systematic review of the literature regarding privacy. We have examined the various competing theories of privacy, and the critiques of those theories. From these competing theories and definitions, we have tried to construct a useful analytical framework.

4 We have called the conceptual approach to privacy that we adopt in this study paper a "core values" approach. It is possible to conceptualise privacy as being a subcategory of two interconnected core values. The first of these core values is the autonomy of humans to live a life of their choosing. The second is the equal entitlement of people to respect. These core values are normative or moral values.

5 We have taken the view that privacy has two main dimensions: informational privacy, and local or spatial privacy. Informational privacy is concerned with control over access to private information or facts about ourselves. The Commission considers that not all personal information can be regarded as private, although opinions may differ as to exactly which facts count as private. Local or spatial privacy is concerned with control over access to our persons and to private spaces, typically in the home but in other places as well. We are able to behave differently in our private space than we do when exposed to the gaze of others. A person's house can be regarded as that person's castle; the home, that person's safest refuge. This is a bedrock principle of the common law.

6 A harm-based analysis is another useful way of looking at privacy. A person's privacy can be harmed by the collection, processing and dissemination of information about him or her, as well as by intrusions into his or her solitude or seclusion. The core values approach and the harms approach can be linked. The first deals with two main dimensions of our expectation that there are areas of our lives over which we are entitled to exert control. The second demonstrates the types of harm against which people should be protected in those areas.

7 Privacy can also usefully be viewed through the lens of risk. Some risks of harm are more serious than others – the more likely a harm is to eventuate, the more serious it will be. The gravity of a possible harm also impacts on a risk's seriousness. A risk-based approach requires risks of privacy infringements to be weighed against possible preventive measures. In some cases, the effort required to guard against a risk may be disproportionate to its seriousness. Under a risk-based approach to privacy, there are three categories of risk:

- risks of injustice;
- risks to personal control over collection of personal information; and
- risks to dignity and embarrassment by disclosure and exposure of information.

8 Various risks to privacy can be identified and weighed to help assess policy frameworks. It is important to realise that different people place different levels of importance on issues of privacy. Some people are unconcerned about privacy and are willing to allow all sorts of information about themselves to be collected. They will give risks to privacy very little weighting. Others are "privacy pragmatists" who may give privacy considerations some weight, but are prepared to make explicit trade-offs in which personal information is provided in return for specific benefits, such as better service or discounts. Others are "privacy fundamentalists" who are unwilling to provide personal information except in situations in which they can exercise a high level of control.

9 It is important that public policy frameworks take into account this range of public perceptions about the importance of privacy. The rationales for privacy protection need to be shaped by concerns about risk and about trust. There needs to be a reasonable degree of consensus in the community in order to produce a stable platform for regulatory policy in this area.

A POLICY APPROACH

10 Privacy is an important and indispensable value in modern civilisation, but the right to privacy is not an absolute right. It has to be balanced against other values. Freedom of expression, which is very important in a democracy, is one of the most prominent of these other values. There are points of tension between privacy and other values, and this needs to be recognised.

11 Privacy and other values need to be weighed and balanced with reference to the particular circumstances in which they arise. Different weights may be appropriate for different values depending on the area of human activity; for instance, land transfer records should be treated differently from individual

health records. The context is everything. The task in front of the Law Commission is to look at privacy in a range of contexts to see what weighting it should be given in each.

12 In some areas, it is clear that the value of privacy will be given a heavy weighting and should be protected by law and policy. For instance, it is widely recognised that there is a need for some regulation of data held by government and the private sector in order to protect information relating to individuals. The main question in this area is how to achieve the necessary protection in an effective manner. This involves choosing the right policy instrument.

13 In other contexts, the importance of privacy relative to other competing values and interests is more debatable. For instance, the emerging tort of invasions of privacy is arranged around a relatively open-textured and undefined framework. Freedom of expression is a value that needs to be given heavy weighting in that framework.

14 In light of this, the Law Commission's view is that it would be a mistake to adopt a broad, comprehensive and all-embracing approach to privacy. Instead, a careful analysis should be conducted of each discrete area in which privacy issues arise. Competing factors must be weighed in specific contexts in order to decide whether legislation is necessary.

15 This approach may look like ad hoc balancing and, in truth, it is. It is our view that this sort of analysis needs to be conducted in each policy area. Otherwise we will end up with an unpredictable, general privacy law of little utility and dangerously uncertain breadth of application.

16 All legislative and judicial decisions represent a balance between competing values and objectives. On some occasions, privacy should weigh heavily in the balance. On other occasions, other countervailing values will be more important. We are saying nothing more profound than that our approach to privacy protection should be piecemeal and particularised, not generalised. Where there are demonstrable problems and abuses, intervention should be made, but not otherwise.

PRIVACY IN NEW ZEALAND LAW

17 In chapter 4 of this study paper, we trace the development of privacy in statute and common law in New Zealand in order to learn how we arrived at our present position. The common law torts of trespass, assault and nuisance, together with various discrete statutory provisions protecting property and prohibiting certain disclosures of information, provide a patchy protection for some aspects of privacy. A range of legal provisions have the ancillary consequence of protecting aspects of privacy, but privacy itself was not specifically mentioned as something that the law protected until the mid-1970s in New Zealand.

18 For many years, the criminal law has regulated certain kinds of privacy invasion through the creation of criminal offences for particular actions or behaviours that impact on individual privacy to an unacceptable degree. For example, in 1927 it was made an offence to be found on property without lawful excuse (although, in that instance, privacy protection was probably incidental to the main purpose of protecting possession of land). In 1960, it was made an offence to peep or peer into the window of a dwelling house. An 1884 Act regulating the telegraph service made it an offence to disclose the contents of any telegram or telegraph. This was extended to letters in 1919.

19 The Danks Committee's report on official information in 1981 contained a list of statutory prohibitions of the disclosure of official information. The list included education information, complaints about safety matters, electoral and polling secrecy, adoption records, prison records, and social welfare information. Many of these restrictions on disclosure were intended to protect individual privacy. By contrast, however, from early times in New Zealand, departments and agencies had been required by law to maintain public registers containing personal information. The general rule in relation to these registers was that they could be searched by anyone.

20 For many years, it has been possible to redress what might be classified as infringements of privacy under some other head of the common law. For instance, assault, battery and negligence can all be used to protect against violations of one's bodily integrity; privacy of the home can be protected via trespass and nuisance; and, depending on the circumstances, personal information can be protected via causes of action such as breach of confidence, negligence, copyright, defamation, malicious falsehood, and the tort of passing off.

Legal recognition of privacy

21 It has taken many years for the common law of New Zealand and other countries with similar legal systems to recognise privacy as a basis for civil action in itself. But social attitudes change over time, and when this happens the law generally recognises that change. Since the mid-1970s, New Zealand has progressively moved to a position where privacy is recognised not only as an important social value but also as one that the law should protect.

22 An important factor in engendering this change has been the rapid advance of new technology. In particular, the storage and processing of personal information by computers has caused an increasing awareness of the need for more generalised privacy protection. Legislation protecting the dignity of the individual, such as the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993, has also increased public awareness of privacy issues.

23 Local privacy has come to be protected in a number of ways. In 1974, it became an offence in New Zealand for a private detective to photograph, or make visual or aural recordings, of a person without his or her consent. The Harassment Act 1997 introduced both civil and criminal penalties for a pattern of conduct such as watching another person's residence, entering a person's property, or making contact with a person by telephone, correspondence, or in any other way. In 2006, it was rendered an offence to covertly film someone while they are in an intimate situation.

24 From the early 1970s, due in part to the growing use of computers, there was an increasing interest in protection of informational privacy, in New Zealand and the rest of the world. For instance, the Wanganui Computer Act 1976 prescribed stringent security measures around the personal information stored in the Wanganui Computer Centre. In 1979, a new part 9A was added to the Crimes Act 1961 titled "Crimes against personal privacy". It includes an offence of using a listening device to intercept someone else's private conversation, a provision which was more recently extended to any form of interception device. Offences relating to computer hacking have also been introduced. The Crimes Act allows

regulated exceptions to such offences for law enforcement purposes. This area involves a careful balancing act between the needs of law enforcement agencies to detect crime and the individual's expectations of privacy.

Privacy Act 1993

25 The Privacy Act 1993 was passed to promote and protect individual privacy in accordance with recommendations of the Organisation for Economic Cooperation and Development, of which New Zealand is a member. The Act was a major initiative aimed at giving substantial protection to informational privacy. It sets limits on the type of information that can be collected, the reasons for collection, the form of collection, and the use of the information. The Privacy Act 1993 is by far the most significant New Zealand law on the subject of privacy, and will be the subject of a full review by the Law Commission in the course of this project.

26 The Act takes a broad view of informational privacy, and sets out principles relating to the collection, storage, security, accuracy, use and disclosure of personal information. These privacy principles apply to information held by both public and private sector agencies. However, the news media and their news activities are exempted from the Act's main principles. The Act's privacy principles are not enforceable in a court; when they are infringed, a complaint can be made to the Privacy Commissioner, and in some cases the matter may be taken to the Human Rights Review Tribunal. The privacy principles in the Act go beyond the protection of autonomy and equality of respect, which are the values protected by privacy under the "core values" approach described in this study paper. The Act also protects individuals against other detrimental uses of their personal information, for instance, for the purpose of identity fraud. The Act includes provisions relating to personal information in "public registers", a topic which will be the subject of a separate report as part of this Review.

The media

27 The media are constrained by certain privacy considerations. The Broadcasting Act 1989 requires broadcasters to maintain standards consistent with "the privacy of the individual". Complaints about breaches of this standard can be made by members of the public and heard by the Broadcasting Standards Authority. The BSA has the power to award up to $5000 compensation in cases where it finds that privacy standards have been breached. Privacy is also protected in some aspects of court reporting, especially in family court cases, and in criminal proceedings there is a judicial discretion to prohibit the publication of identifying details.

Tort of invasion of privacy

28 In 2004, the New Zealand Court of Appeal recognised a tort of breach of privacy (that is, a civil court action alleging that a person's privacy has been invaded). It had two fundamental requirements. First, the existence of facts in respect of which there was a reasonable expectation of privacy. Secondly, publicity given to those private facts that would be considered highly offensive to an objective reasonable person. The court also said there should be a defence according to which publication could be justified by a legitimate public concern in the information. So far, this tort extends only to the publication of private facts,

and so protects informational privacy only. However, it remains open that the courts could decide in the future to extend the tort to cover intrusions into seclusion, such as surveillance.

New Zealand Bill of Rights Act 1990

29 There is no express constitutional guarantee of the right to privacy in New Zealand. Considerations of privacy can arise under sections 5 or 21 of the New Zealand Bill of Rights Act 1990: under section 5 as a justifiable limitation on rights protected by the Act; or under section 21, as a value underlying that section's protection from unreasonable search and seizure by State enforcement agencies. However, privacy itself is not an express right under the Bill of Rights Act. Section 28 provides that an existing right or freedom is not abrogated or restricted because it is not included or not fully included. However, any Bill of Rights analysis under sections 5, 6 or 7 of the Act is to be performed with respect to the rights and freedoms contained in the Act. This suggests that rights and freedoms expressly contained in the Act have a different status than rights and freedoms that are excluded, notwithstanding section 28.

SOCIAL ATTITUDES

30 Attitudes to privacy do not exist in a vacuum. Chapter 5 of this study paper looks at how attitudes to privacy are shaped by history, culture and personal experience. As a consequence of this, they vary widely across historical periods and cultures, and between different individuals and social groups. In this study paper, we explore past and present attitudes to privacy and the implications of these attitudes for law and policy. Examining the history of privacy helps us to understand that its meaning is not fixed, but changes over time.

31 It is often assumed that privacy is under unprecedented threat in today's world. Since the late 19th century, concerns about the loss of privacy have been closely linked with developments in technology. However, if this threat is fairly recent, the expected privacy levels that it threatens are also quite recent. The levels of privacy we now enjoy have probably only existed for a few generations at most. Many people in earlier generations had little physical privacy, and there was no general expectation of privacy in personal communications until relatively recently. The development of modern Western ideas of privacy is closely linked to the emergence of the concept of the self-contained individual. Boundaries of the public and private have also shifted over time. More kinds of information, and more physical spaces, have come to be regarded as private.

Māori and privacy

32 One important element of the social context in which privacy should be assessed in New Zealand is Māori culture. There has been little specific research to date regarding te ao Māori (the Māori dimension) and privacy, and more work is required.

33 A number of Māori customary concepts have parallels with or relevance to concepts of privacy. Respect for the mana (personal power or standing) of each individual is central to Māori and other Polynesian cultures, and is consistent with the "core value" of the equal entitlement of all persons to respect which we have referred to above. The key Māori concepts of tapu (which can be defined as "set apart under a ritual restriction") and noa (a state of being free from such restrictions) are also relevant to privacy, as is the concept of

whakamā (a state of being associated with feelings of inadequacy and hurt and with behaviour marked by withdrawal from communication with others). None of these concepts, however, can be directly equated with the English words "privacy" or "private".

34 There are also likely to be distinct Māori perspectives on what constitutes a private place and private information. For instance, although much business that takes place on a marae may be "public", it is not necessarily a public place for people who do not belong to that marae. Complex questions can also arise regarding the types of information that Māori consider private, and to whom that information belongs. It may be considered that some types of information belong not to individuals but to a group. This is particularly likely to be true of whakapapa (genealogical) information.

35 The relationship between Māori customary concepts and the concept of privacy is not a straightforward one, nor is it easy to assess what influence such concepts have on Māori attitudes to privacy today. Such concepts and values may be useful, however, in making privacy law more relevant to tikanga Māori. Te ao Māori is an important dimension of the New Zealand social fabric, and should be reflected in our legal treatment of privacy.

Age and privacy

36 Age is another social factor likely to influence attitudes to privacy. People generally have different understandings and expectations of privacy at different ages and stages of their lives. Young children generally have very little privacy and are under parental surveillance most of the time. At the other end of life, old people may lose much of their privacy if they become sick or disabled, particularly if they move into residential care. Different generations may have different attitudes to and concepts of privacy because they have grown up in different worlds. Today's young people have grown up in a world in which the internet, mobile phones and text messages allow them to keep in touch with their friends constantly. They use these technologies to form, develop, and maintain friendships. This experience of constant connectivity may mean that their ideas about limiting access to themselves and to information concerning them are different from those of older generations.

37 Blogging and online social networking have also changed things enormously. Large numbers of young people use the internet. Many of them use social networks and post profiles online. These profiles often contain names, photographs and personal information. The activities of the young online have led to claims of a generation gap, and the older generation tends to look on these developments with alarm and misapprehension. Young people have been portrayed as recklessly honest or uninhibited online, and some say that privacy is threatened by this new behaviour. However, there is also evidence that young people do exercise some caution about the information they make available about themselves online. It is very difficult to know whether apparent differences in attitudes and behaviour between younger and older generations herald a long-term shift in views of privacy. Only time and long-term research can answer these questions.

Public opinion

38 Measuring social attitudes to privacy has its difficulties. There is a significant body of international research regarding public attitudes to privacy, and how those attitudes can be gauged, which indicates that there can be problems and limitations with studies of public opinion on privacy. However, public opinion surveys can play a useful part in policy debates if these problems are borne in mind.

39 The Office of the Privacy Commissioner and the Broadcasting Standards Authority have both conducted surveys of attitudes to privacy in New Zealand. Details of these surveys are set out in the main body of this study paper. While it is difficult to draw firm conclusions from the surveys, a number of reasonable inferences can be drawn. For instance, a majority of New Zealanders surveyed said they were concerned about privacy in general terms and desired that their personal information be kept private. Opinion varied regarding the importance of privacy in specific contexts, and there was also some divergence in attitudes according to gender, age, ethnicity and socioeconomic background.

TECHNOLOGY

40 Technology and technological change can have profound implications for privacy and privacy-related law reform. These implications are considered in chapter 6 of this study paper. The Law Commission's Review is in part a response to the technological developments that have occurred since the passing of the Privacy Act 1993. Extraordinary technological developments have occurred in those years, relating to computer technology and the rise of the internet; and also encompassing other technologies, such as technologies of visual and audio surveillance and location detection; and biometric, genetic and brain-scanning technologies. These technologies are very useful and can have positive results for society and individuals. But they also have the potential to be used in such a way as to invade or curtail privacy.

Computer technology

41 Concerns about the implications for privacy of the aggregation of personal information in computer databases first emerged in the late 1960s and early 1970s. Concerns that such information could be used for purposes other than those for which it was originally provided, or that information could be disclosed to a third party without the knowledge or consent of the person to whom it related, remain very real today.

42 In addition to these concerns from an earlier phase of the information age, rapid advances in computer technology since the 1970s have created new privacy challenges and heightened old ones. Today's computers are more powerful, cheaper, have greater memory, and are faster than ever before. The standard desk-top computer today is more powerful than the most expensive supercomputer of ten years ago. An average cell phone today is at least as powerful as a personal computer from a decade ago. New kinds of data can be stored cheaply in large volumes.

Data collection and analysis

43 These advances in computing have made it possible to extract, collate and analyse data in powerful and sophisticated ways that have significant implications for informational privacy. Two key techniques that are greatly facilitated by more powerful computer technology are used by both public and private sector organisations: data matching and data mining. Data matching involves comparing data that comes from different sources and has been collected for different purposes. The general aim is to find data that relates to the same person for purposes such as detecting errors or fraud, locating particular individuals, and determining eligibility for government benefits. Data mining involves extracting information that is implicit in data sets, usually by discovering new relationships among the data elements.

44 Both data matching and data mining can raise privacy concerns for a number of reasons. They involve the use of personal data for purposes other than those for which it was collected, and they seek to uncover previously unknown information about people. Errors or incomplete information can be repeated and their effects multiplied. These processes can be carried out without the knowledge or consent of the subject of the information.

The internet

45 The growth and development of the internet is a major element of the technological change that has occurred since the Privacy Act 1993 was passed. The internet is a type of super network, a worldwide collection of interconnected computer networks based on a set of standard communication protocols. Over recent years, it has transformed many aspects of our lives.

46 The internet has a number of notable characteristics that make it difficult to control, or to trace the flow of data within it. It has no borders – it is not physically located in any one state and can be accessed from anywhere. It is not centrally owned or controlled. It is interactive and dynamic. As a result, the internet has given rise to new and difficult privacy issues.

47 Our study paper focuses on two broad themes with regard to the internet's impact on privacy: first, the collection of personal information by companies that track and record users' online habits and activities; and secondly, the online availability of personal information posted by private individuals. The first category of information collection can be done overtly by asking users to register for a particular website and provide certain personal information. There is clearly some knowledge and consent on the user's part in such cases.

48 Alternatively, however, it is possible for companies to collect information about a user without the user's knowledge or consent. This covert collection is of greater concern from a privacy perspective and can be done in a number of ways. One such method is that websites can collect information about a user's internet service provider (ISP), internet protocol (IP) address, computer software and hardware as that user navigates the site. Information can also be collected about how users interact with a site, and which other website they linked from. Similarly, internet search companies collect information about the search terms users enter when conducting searches. This kind of information is often used to target advertisements to particular users.

49 The second area of particular concern is the posting of various forms of personal information, particularly images, on the internet by private individuals. The phenomena of blogging and online social networking involve individuals posting information about themselves and others. The online posting of information about others without their consent can have significant privacy implications. The availability of images of people on the internet gives rise to fears because such images can easily be disseminated widely and viewed by many people. They can be stored permanently, viewed repeatedly and subject to close scrutiny. They can also be doctored electronically or taken out of context and given new meanings, including embarrassing, derogatory or sexualised meanings.

50 Other kinds of information posted on the internet also falls into this category. Online mapping services that provide photographic bird's-eye views of locations raise privacy concerns as individuals' houses can be identifiable. More recently, Google's Street View service has raised concerns as it provides 360-degree views from street level of some United States cities, allowing individuals to be seen. In short, the internet makes it possible to widely distribute information about individuals without their consent in ways that would not otherwise be possible.

Implications of the internet for privacy law

51 A number of legal issues relate specifically to the impact of the internet on privacy. First, there are jurisdictional issues – the internet is without borders and can be accessed anywhere in the world. Secondly there are enforceability issues – it can be difficult to determine the respective liabilities of various parties regarding material posted on the internet that breaches privacy. Numerous people may be involved to varying degrees, from the person who posted the information originally, to people who link to the page from other websites, to the ISP and so on. There are also particular issues relating to the Privacy Act 1993. The Act was not drafted with issues related to the internet in mind. Some of its language is ambiguous with regard to how it applies to internet publication, and some defined terms may benefit from being updated with the internet in mind.

Surveillance and location technologies

52 The technology relating to surveillance has also rapidly progressed in recent times. It has been said that society is moving from "traditional surveillance" to the "new surveillance". Traditional surveillance involves the conscious, targeted surveillance of individuals by powerful institutions, using cameras for instance. The new surveillance is constant, is often not deliberate or targeted, and can be carried out by almost anyone using devices that are becoming smaller, cheaper and less noticeable. Such devices are increasingly widely used, and are often networked. Ultimately, they may become ubiquitous, so that everyone can expect to be photographed, monitored by wireless sensor networks, or otherwise under surveillance in public, or perhaps even in private places. Concern has been expressed that we may adjust our expectations of privacy in light of this ubiquitous surveillance.

Technologies of the body

53 The final set of new technologies discussed in the study paper are technologies that allow us to identify, or unlock the secrets of, the human body itself. Advances in biometrics allow individuals to be identified by finger or iris scanning, and facial, voice and gait recognition. Genetic science has allowed us to map the human genome. We can now unlock genetic information about people that many would consider to be intensely private, for instance, information about individuals' predisposition to certain diseases. Brain-scan technology and psychological testing also raise potential privacy concerns. Our improved understanding of brain function may threaten the privacy of a person's inner thoughts, which should be the ultimate refuge from the outside world.

Privacy-enhancing technologies

54 Our study paper also recognises that new technologies can be used to protect or enhance privacy. Such privacy-enhancing technologies (PETs) can either be used by individuals to protect their own privacy, or built into technologies at the design stage to ensure that they protect privacy. It is not suggested that PETs will provide solutions to all privacy problems, or even to all privacy problems that themselves directly stem from technology. However, they can be used as part of a law reform programme to supplement and complement other regulatory approaches, as well as being used as conditions or standards specified in other forms of regulation.

55 New technologies can play enormously beneficial roles in individuals' lives, and in the operation of society as a whole, but they can also be used in ways that threaten privacy interests. The challenge is to find ways to enjoy the benefits of these technologies, while also minimising or eliminating the risks they pose to privacy.

THE INTERNATIONAL DIMENSION

56 The international dimension of privacy is of vital importance and is addressed in chapter 7 of the study paper. An enormous amount of personal information is transferred across borders, and there are a number of international instruments that bear on privacy issues.

Privacy as a human right

57 Privacy has been expressed internationally as a human right. Article 17 of the International Covenant on Civil and Political Rights, to which New Zealand is a party, provides that:

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

The implications of these obligations are discussed in the study paper.

Organisation for Economic Cooperation and Development

58 The Organisation for Economic Cooperation and Development (OECD), to which New Zealand belongs, is an important contributor to managing privacy concerns at an international level. The OECD has worked out standards that have been designed to harmonise the laws of various countries on the subject of

personal data protection. The OECD Council adopted the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980. The guidelines apply to personal data whether in the public or private sectors, and set out a number of important principles for the handling of personal data. These principles are reflected in New Zealand's Privacy Act 1993.

59 In 1985, a declaration on trans-border data flows was adopted by Ministers of OECD member states, in order to engage with issues arising from the "rapid technological developments in the field of information, computers and communication". More recently, the OECD Council adopted a recommendation in 2007 urging greater cross-border cooperation among member states in the enforcement of privacy laws.

Asia Pacific Economic Cooperation

60 Another international development of importance to New Zealand is that the Asia-Pacific Economic Cooperation (APEC) group has developed a set of principles relating to informational privacy. APEC has 21 member economies, including New Zealand. The APEC principles have been criticised as being weaker than those of the OECD, but work is continuing within APEC on the development of cross-border privacy rules with the aim of protecting individuals' personal information no matter where that information is transferred or accessed within the APEC region.

European Union and United States of America

61 The European Union directive of 1995/46/EC of the European Parliament and of the Council, dated 24 October 1995, provides protection for individuals with regard to the processing of personal data. Member States of the European Union have proceeded to implement that directive, and the United Kingdom implemented it though the enactment of the Data Protection Act 1998.

62 The United States takes a different approach to privacy from that taken by the European Union, and has no comprehensive privacy laws governing the processing of personal information in the private sector. Consequently, there has been an attempt to find a way of bridging these different approaches. Negotiations between the EU and the United States developed a "safe harbour" framework which was approved by the European Union in 2000. The safe harbour regime is intended to assure European Union organisations that a United States company certified to the scheme provides adequate privacy protection as defined by the European Union data protection directive.

Privacy and New Zealand's place in the world

63 New Zealand is a trading nation. It is important for New Zealand businesses to understand the principles governing the handling of personal information in the various jurisdictions with which they trade. This is why the international standards discussed in this section are important. Privacy has become an increasingly trade-related question in terms of the trans-border flow of data, and New Zealand would ignore these international trends at its peril. All law reform proposals in the privacy area need to take them into account. Like other countries, New Zealand also faces significant challenges of enforceability of privacy laws in a context in which personal information is routinely transferred across borders, or posted on websites hosted outside New Zealand.

SOME PRIVACY ISSUES

64 The final chapter of this study paper focuses on a number of remaining issues relating to privacy that the Commission regards as important.

Balancing privacy with other values

65 There are few absolute values in law, and privacy is not one of them. Expectations of privacy are relative and must be balanced against other countervailing values. The balancing is particularly difficult because in some contexts there is a strong public interest in the maintenance of values that can limit or override privacy. One important value that is often in tension with privacy is freedom of information. The balancing of freedom of information and privacy is far from simple. There is no golden rule available to solve the problem, and people will differ on the appropriate balance.

66 The way in which the balancing process is carried out in relation to privacy is, therefore, a matter of prime importance. The key actor in decision-making is the law-maker – in most cases Parliament. The balancing exercise places a considerable burden on the decision-maker to work out what the public interest requires. That may vary with time and place. In marginal cases, there is likely to be considerable room for disagreement.

Persons and privacy

67 Different groups of people may require different levels of protection. Children and young persons may have different attitudes to privacy from their elders, and are regarded as being more vulnerable. Māori may have a different attitude to privacy from the majority of the community, as may other ethnic groups.

68 Whether a deceased person can have a privacy interest is an interesting issue. The Official Information Act 1982 assumes that deceased persons can have privacy, whereas the Privacy Act excludes information about deceased persons from the definition of personal information. Another issue that seems to be unsettled is whether corporations can have privacy rights. This uncertainty reflects the general uncertainty about the concept of privacy itself.

Privacy and the media

69 The interaction between privacy and the media is an issue of vital importance. The guarantee of freedom of expression in the New Zealand Bill of Rights Act 1990 includes freedom of the press, but that freedom is not absolute or uncontrolled.

70 There are a number of restrictions on obtaining information that restrain not just the media but everyone else as well. However, these restrictions are piecemeal and strangely incomplete: it is unlawful to record an oral conversation unless you are a party to it, but it is not unlawful to film people without their knowledge unless they are in an intimate situation.

71 Restrictions on publication are imposed by various elements of the law. It has been suggested that there is a growing tendency in the courts to grant name suppression, particularly interim name suppression, to persons charged with the commission of criminal offences. The language of privacy and its emphasis on the dignity of the individual is now finding a place in some of the judgments of the courts in this area.

72 The development in New Zealand of a tort of invasion of privacy is a further issue that the Commission will be considering in the course of this Review, and one which has implications for the media. There are some uncertainties in the very texture of the tort, and many open questions. Will the tort extend to protect local privacy by, for example, controlling the use of hidden cameras? Will corporations be able to plead it? Must the plaintiff be identified in the publication? Can a privacy claim provide a remedy against false allegations? There is much working out still to be done, and that worries the media. These issues need to be settled, and will be addressed by the Commission in the next phase of the Review.

73 Privacy standards in the broadcast media are regulated by the Broadcasting Standards Authority, which can (among other remedies) award compensation for invasions of privacy. Complaints about breaches of privacy in the print media can be made to the Press Council. While the print media and the broadcast media are regulated in different ways, there is no body charged with maintaining privacy standards on the internet. Content is published on the internet without legal advice or editorial control in many instances. Enforcement is a common problem, particularly if the host of the website is overseas and therefore outside New Zealand's jurisdiction.

74 There are a number of other issues in this area, such as how much privacy there can be in a public place, and the privacy rights of children who are the subject of media coverage.

Privacy and health

75 Privacy in the health system raises a lot of difficult issues. Information is an important ingredient in good health care. The digital revolution has enabled new ways to collect and store health information to ensure it is available to health professionals when they need it.

76 The Privacy Act 1993 applies to protect the privacy of patients and the Privacy Commissioner has issued a Health Information Privacy Code. The central issue for health information is to achieve a proper balance between keeping personal health information confidential and getting the right information to the right person, at the time when it is needed. There needs to be some explicit understanding as to how patient information is to be used once it is collected. Patients need to know how their information may be used, and their concerns need to be addressed. Mental health is a particularly difficult area for privacy protection. There are also emerging issues relating to genetics and medical research.

77 A clear framework is needed on the following issues:

- who may gather personal health information;
- who may use it, for what purposes and under what conditions;
- how the information may be communicated within the health system, and subject to what protections;
- how the information may be held, and by whom; and
- how information may be used by health researchers.

This is an area that may need further attention, and will be examined by the Commission in its ongoing work.

Surveillance

78 The privacy literature is replete with references to surveillance, which involves watching someone in a purposeful and focused way. Surveillance is carried out by a variety of technological devices, and can infringe both local and informational privacy.

79 Law enforcement activities rely heavily on surveillance, and the Law Commission has produced a report on the search and surveillance powers of law enforcement officers. The Commission's recommendations in that report are before the Government, and it is likely that the future shape of the law governing surveillance by law enforcement officers will influence the approach taken to wider issues of surveillance. By going through a number of examples of different types of surveillance it can be demonstrated that the protections in the existing law are patchy and inconsistent. The subject of surveillance will need to be carefully considered in the next phase of the Commission's work.

Privacy and the workplace

80 There are some important issues about the degree to which employees may be placed under surveillance by their employers, and for what purposes this may be done. The study paper examines some proposed and existing legislation on workplace surveillance in Australia. It may be that some fresh regulation in this area is needed in New Zealand, but it probably does not need to be extensive.

Conclusion

81 There are a range of other issues that the Commission will probably need to consider in later stages of the Review, including misunderstanding and misuse of the Privacy Act, whether the proper balance is being struck between enabling information sharing and protecting privacy, and issues relating to direct marketing and credit reporting. All of the issues discussed in this section raise important and often difficult questions about how privacy should be balanced with other interests. This will be one of the major challenges to be discussed in the subsequent stages of the Review.

Chapter 1: Introduction

1.1 It has become common over the past decade to portray privacy as being under threat. Indeed, an internet search of the words "end of privacy" or "death of privacy" will produce a list of books, articles and television programmes suggesting that, if privacy is not already dead, it is very unwell and the prognosis is grim.[1] The Information Commissioner in the United Kingdom has warned that his country is "sleepwalking into a surveillance society", and his words have been echoed in New Zealand.[2] On the other hand, some commentators argue that we have too much protection of privacy in some areas, and that privacy law threatens other important values. These values include freedom of speech and the public's right to information,[3] as well as personal and national security.[4]

1.2 In light of such concerns, the Law Commission considers it timely to review the law relating to protection of privacy in New Zealand. This study paper forms the first part of a four-stage review of New Zealand privacy law ("the Review") being undertaken by the Commission. The Review will consider the adequacy of existing law to deal with perceived threats to privacy, as well as whether legal protection of privacy may be adversely affecting other social values. The present chapter introduces the Review, then explains the purpose and structure of this study paper.

THE LAW COMMISSION REVIEW OF PRIVACY

1.3 The Privacy Act 1993 is now almost 15 years old. Since it was enacted there has been no major review of privacy law in New Zealand. Those reviews that have taken place have focused on the existing Privacy Act, rather than going back to first principles or considering the wider field of privacy law (including the

1 See for example "The End of Privacy" (1 May 1999) *The Economist*; Charles J Sykes *The End of Privacy: The Attack on Personal Rights – at Home, at Work, On-Line, and in Court* (St Martin's Press, New York, 1999); Reg Whitaker *The End of Privacy: How Total Surveillance is Becoming a Reality* (New Press, New York, 2000); Simson Garfinkel *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly, Sebastapol (Calif), 2000); Michael Froomkin "The Death of Privacy?" (2000) 52 Stan L Rev 1461; John Stossel, Audrey Baker and Gena Binkley "The Death of Privacy: With Cameras Everywhere, is Privacy a Thing of the Past?" (7 February 2007) *20/20* ABC News www.abcnews.go.com/2020 (accessed 23 September 2007). Predictions of privacy's demise are not new, however: see Jerry M Rosenberg *The Death of Privacy* (Random House, New York, 1969).

2 Patrick Crewdson "Sleepwalking into a Surveillance Society: Kiwis Face Everyday Spying" (10 April 2007) *The Dominion Post* Wellington A1.

3 See for example Joanne Black "Age of Intrusion" (25 June-1 July 2005) *The Listener* New Zealand 14; Karl du Fresne "Births, Deaths and Other Secrets" (20 April 2007) *The Dominion Post* Wellington B5.

4 For two perspectives from the United States on the privacy vs security debate see KA Taipale "Privacy vs Security? Security" and Marc Rotenberg "Privacy vs Security? Privacy" (9 November 2007) www.huffingtonpost.com (accessed 12 November 2007).

common law).[5] There have been a number of developments over the past 15 years that, in the Commission's view, warrant a more wide-ranging review of New Zealand privacy law:

- There have been rapid advances in technologies that have an impact on privacy. In particular, the spectacular rise of the internet raises new issues for the protection of privacy.
- There have been developments in the regulation of privacy internationally. New technologies have facilitated the flow of data across borders, so that privacy of personal information cannot be considered solely at the national level.
- In part due to technological developments, state agencies are seeking to collect and use personal information in new ways for purposes such as service delivery and law enforcement.
- The Court of Appeal decision in *Hosking v Runting* has found that there is a tort of invasion of privacy in New Zealand common law.[6] There have also been developments in the common law relating to privacy in other jurisdictions.
- New Zealand has experienced significant social and cultural changes which may have led to changes in social attitudes to privacy.

1.4 The Commission has therefore received a reference to undertake a major review of privacy law, to proceed in four stages. The terms of reference for the Review appear at the front of this study paper. This study paper is the outcome of stage 1 of the Review, in which the Commission has undertaken a policy overview of privacy values, changes in technology and international trends, and assessed their implications for New Zealand law. Stage 2 is a review of the law relating to public registers, and the Commission will be reporting on whether this law should be altered as a result of privacy considerations and emerging technology. In stage 3 the Commission will report on the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy, while in stage 4 the Commission will review the Privacy Act 1993 with a view to updating it. Stages 1 and 2 have been conducted in tandem, while stages 3 and 4 will be commencing early in 2008.

1.5 For the later stages of the Review, issues papers will be produced and made available on the Commission's website, and the Commission will call for submissions on the options put forward in those papers.[7] On the basis of the submissions received, the Commission will formulate its recommendations and its final reports will be tabled in Parliament. The four stages of the Review should be considered as parts of a larger whole, and it will be important to read the four volumes in conjunction with each other.

RELATED WORK

1.6 Although this Review is the Commission's first major inquiry into the whole field of privacy law, it has previously examined aspects of law relating to privacy in New Zealand. The Commission will also have the benefit of taking into account valuable work on privacy being undertaken by other agencies in New Zealand and overseas.

5 Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review* (Office of the Privacy Commissioner, Auckland, 1998); Mai Chen *Scoping Paper on the Privacy Act 1993* (prepared for the Hon Margaret Wilson, Associate Minister of Justice, 2001).

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

7 An issues paper for stage 2 has already been released: New Zealand Law Commission *Public Registers: Review of the Law of Privacy: Stage 2* (NZLC IP3, Wellington, 2007).

Previous Law Commission projects

1.7 A sub-committee of the Law Revision Commission, the predecessor to the present Law Commission, produced one of the earliest reports on privacy in New Zealand in 1973. That report, which focused on computer data banks, recommended the establishment of an independent agency to oversee the collection and handling of personal information in computer data banks in both the public and private sectors.[8]

1.8 The present Law Commission has produced a number of publications that are relevant to privacy, including those on:

- *Electronic Commerce*;[9]
- *Protecting Personal Information from Disclosure*;[10]
- *Intimate Covert Filming*;[11]
- *Access to Court Records*;[12] and
- *Search and Surveillance Powers*.[13]

1.9 The Commission's *Search and Surveillance Powers* report (2007) looks at the law governing the search and surveillance powers of police and other law enforcement agencies. It discusses privacy as the key human rights value implicated by such powers.[14] Privacy issues in relation to search and surveillance by law enforcement agencies are therefore excluded from the Commission's Review of privacy. The privacy implications of surveillance by other organisations, and by private individuals, do fall within our terms of reference, however.

Australian law reform projects

1.10 Three Australian law reform commissions currently have projects looking at aspects of privacy. The New Zealand Law Commission is following these projects closely, and working cooperatively with the Australian commissions.

Australian Law Reform Commission (ALRC)

1.11 The ALRC, the federal law reform body, is undertaking a review focusing on the extent to which the Privacy Act 1988 (Cth) and related laws continue to provide an effective framework for protection of privacy in Australia. The ALRC has already produced two issues papers and a discussion paper as part of this inquiry,[15] and is due to submit its final report to the Commonwealth Attorney-General by 31 March 2008.

---

8 Law Revision Commission *Report of Sub-Committee on Computer Data Banks and Privacy* (1973) 36-37.

9 In three volumes: New Zealand Law Commission *Electronic Commerce* (NZLC R50, Wellington, 1998); (NZLC R58, Wellington, 1999) ch 11; (NZLC R68, Wellington, 2000) ch 5.

10 New Zealand Law Commission *Protecting Personal Information From Disclosure* (NZLC PP49, Wellington, 2002).

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

12 New Zealand Law Commission *Access to Court Records* (NZLC R93, Wellington, 2006) especially 54-56, 125-130.

13 New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007).

14 Ibid, 38-40.

15 Australian Law Reform Commission *Review of Privacy* (ALRC IP31, Sydney, 2006); Australian Law Reform Commission *Review of Privacy: Credit Reporting Provisions* (ALRC IP32, Sydney, 2006); Australian Law Reform Commission *Review of Australian Privacy Law* (ALRC DP72, Sydney, 2007).

New South Wales Law Reform Commission (NSWLRC)

1.12 The NSWLRC conducted a review of the law relating to surveillance, culminating in a final report completed in 2005.[16] It subsequently received a reference to inquire into privacy law more generally, including the desirability of a consistent legislative approach to privacy in a number of New South Wales statutes and the desirability of introducing a statutory tort of privacy in New South Wales. The NSWLRC has so far produced a consultation paper focusing on the possible introduction of a statutory cause of action for invasion of privacy.[17] A second consultation paper on other aspects of privacy will follow, and a final report is expected in early 2008.

Victorian Law Reform Commission (VLRC)

1.13 The VLRC's privacy reference covers two specific issues: workplace privacy and surveillance in public places. A final report on workplace privacy was published in 2005.[18] A consultation paper on surveillance in public places is expected in early 2008, with a final report to be produced by the end of 2008.

Other law reform commissions

1.14 The Hong Kong Law Reform Commission produced the last of a series of reports on aspects of privacy in 2006.[19] The South African Law Reform Commission has a current project on privacy and data protection, which has so far produced an issue paper and a discussion paper.[20] The British Columbia Law Institute is currently reviewing the Privacy Act of British Columbia (which creates a statutory tort of violation of privacy) and has released a consultation paper on this topic.[21]

New Zealand Government

1.15 The Ministry of Justice is undertaking work on modernising the Privacy Act 1993, with a view to making a number of operational and technical amendments to the Act. This work is more limited in scope than the Commission's Review. It is anticipated that the Act will have been amended before the Commission completes its Review, and that the Commission will be able to take these amendments into account in its own recommendations for reform of the Act.

---

16 New South Wales Law Reform Commission *Surveillance: Final Report* (NSWLRC No 108, Sydney, 2005); this report should be read in conjunction with the more detailed *Surveillance: Interim Report* (NSWLRC No 98, Sydney, 2001).

17 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007).

18 Victorian Law Reform Commission *Workplace Privacy: Final Report* (VLRC, Melbourne, 2005).

19 Hong Kong Law Reform Commission *Report on Reform of the Law Relating to the Protection of Personal Data* (1994); Hong Kong Law Reform Commission *Report on Privacy: Regulating the Interception of Communications* (1996); Hong Kong Law Reform Commission *Stalking: Report* (2000); Hong Kong Law Reform Commission *Civil Liability for Invasion of Privacy: Report* (2004); Hong Kong Law Reform Commission *Privacy and Media Intrusion: Report* (2004); Hong Kong Law Reform Commission *Privacy: The Regulation of Covert Surveillance: Report* (2006).

20 South African Law Reform Commission *Privacy and Data Protection* (SALRC Issue Paper 24, Pretoria, 2003); South African Law Reform Commission *Privacy and Data Protection* (SALRC Discussion Paper 109, Pretoria, 2005).

21 British Columbia Law Institute *Consultation Paper on the* Privacy Act *of British Columbia* (Vancouver, 2007). The Institute is the effective successor to the Law Reform Commission of British Columbia, but is not a government-created body.

1.16 There is also work going on in other government departments that is relevant to privacy. Of particular note is the e-government programme being coordinated by the State Services Commission.[22] This programme aims to make government information and services more accessible through the use of technology. Protecting privacy is a key consideration in this programme.

STAGE 1 OF THE LAW COMMISSION REVIEW

1.17 The Commission's aims in stage 1 of this Review have been to:

- provide a conceptual framework for the Review by examining different theories of privacy and formulating an approach to privacy that seems appropriate for the Review;
- review developments that have an impact on privacy, with a particular focus on social attitudes and values, emerging technologies and international trends;
- identify some key issues for further exploration in the later stages of the Review; and
- identify the implications for New Zealand civil, criminal and statute law of the Commission's conceptual approach to privacy and its review of developments affecting privacy.

1.18 This study paper is based primarily on a review of the literature on privacy. We have also engaged in preliminary consultation with interested parties and privacy experts. The Law Commission and the Office of the Privacy Commissioner jointly organised a general forum on privacy issues in May 2007, and a forum on health and privacy in August 2007. In addition, the Commission held a meeting with people working in the media and related fields in July 2007. Meetings have also been held with a range of other interested organisations and individuals. The Commission has found these meetings very useful for gathering information and hearing a range of perspectives on privacy. We intend to consult further as we move into stages 3 and 4 of this Review. In particular, we will need to consult with interested parties about specific ways in which privacy law should be reformed. The Commission has also established a reference group of academic experts on privacy law and policy to provide advice and comment as required.[23]

Commenting on this study paper

1.19 Because this is a general background paper for the Review, it does not include recommendations. For this reason we have not published it in draft form or called for submissions on its content. The issues papers produced for the later stages of the Review will refer back to matters discussed in this study paper, and it may therefore be necessary to comment on this study paper in submissions on the issues papers. Should individuals or organisations wish to comment separately on this study paper, the Commission would welcome comments, which should be sent to the address given at the front of the paper.

22 www.e.govt.nz.

23 The members of the reference group are: Ursula Cheer (University of Canterbury); Miriam Lips (Victoria University of Wellington); Selene Mize (University of Otago); Nicole Moreham (Victoria University of Wellington); Steven Price (Victoria University of Wellington); Paul Roth (University of Otago); Rosemary Tobin (University of Auckland).

Structure of the stage 1 study paper

1.20 Following this introduction, chapter 2 looks at theories of privacy. It assesses the strengths and weaknesses of the various ways in which privacy has been defined and conceptualised; summarises key features of the "privacy paradigm" underlying law and policy in this area, and critiques of the paradigm; and distinguishes privacy from certain related concepts. We then set out our own conceptual approach to privacy in chapter 3. We argue that privacy is a sub-category of the values of autonomy and equality of respect, and that it has two main dimensions: informational and local or spatial. We also consider how an approach to privacy that focuses on classifying types of harms and risks might be relevant to the Commission's conceptual framework. Having established the conceptual framework for our Review, we examine the legal framework in chapter 4. This chapter takes a broadly historical approach, looking at the emergence of privacy as an explicit value in the law in the last quarter of the 20th century.

1.21 The middle section of the study paper looks at the implications for privacy of developments in social attitudes, technology and the international legal dimension. Chapter 5 is concerned with the ways in which attitudes to privacy may vary over time and between different social groups. It briefly reviews the history of privacy in the West; discusses cultural perspectives on privacy (particularly Māori perspectives); considers whether today's young people may understand privacy differently from previous generations; and examines opinion poll data about New Zealanders' attitudes to privacy. In chapter 6 we focus on the ways in which technological change is affecting privacy, and on some implications of such change for privacy law. New and emerging technologies have the potential to threaten privacy in a variety of ways, but technology may also provide means of protecting privacy. Chapter 7 then situates privacy law in its international context. It considers privacy in international human rights law; the data protection principles of the Organisation for Economic Co-operation and Development, the Asia-Pacific Economic Co-operation group, and the European Union; the implications of international trade rules for informational privacy; and problems of cross-jurisdictional enforcement.

1.22 We conclude this study paper with a preliminary examination in chapter 8 of some key privacy issues that we intend to explore further in stages 3 and 4 of the Review. We discuss the balancing of privacy against other values; issues concerning certain categories of "person" in privacy law; privacy and the media; privacy and the health system; surveillance; and workplace privacy. At this stage we put forward no definite views about these issues, but raise some questions and concerns that may give rise to a need for reform of current legal frameworks.

1.23 Privacy is a complex and multifaceted topic, and we do not claim that this study paper is a comprehensive review of the subject. We hope, however, that this paper not only provides a sound framework for the Commission's Review, but also acts as a useful introduction to privacy for readers without specialist knowledge in this area.

Chapter 2:
Theories of Privacy

2.1 Privacy is notoriously difficult to define, so it is little wonder that there are many competing definitions of, and ways of thinking about, this elusive concept. This chapter surveys some of them. We start by looking at how various theorists have defined and conceptualised privacy. We then outline some key features of what has been called the "privacy paradigm", a set of assumptions that underlie much of the law and policy in relation to privacy protection. We also consider some critiques of the privacy paradigm. Finally, we look at how privacy may be distinguished from certain related or overlapping concepts: secrecy, confidentiality, reputation and property.

CONCEPTUALISING PRIVACY: SOME THEORIES

2.2 In this section we set out the main schools of thought in relation to how privacy is best conceptualised and defined, and some of the grounds on which each approach has been criticised. Our summary of the theories draws on a number of useful surveys of the literature on privacy by other authors.[1] This review is by no means exhaustive. It is also important to bear in mind that these various conceptions are not necessarily mutually exclusive, and most writers combine elements of several different conceptions.

2.3 One broad division among privacy theorists is between those who believe that a coherent "core" or "essence" of privacy can be identified and those who consider that no common core of shared characteristics links the various interests that are grouped under the label of privacy. Most of the theories outlined below are attempts to construct a coherent definition or conception of privacy, but the reductionist and pragmatic approaches abandon the search for privacy's core, albeit for different reasons.

1 Daniel Solove "Conceptualizing Privacy" (2002) 90 Cal L Rev 1087; Judith DeCew "Privacy" in Edward N Zalta (ed) *Stanford Encyclopaedia of Philosophy* (Winter 2006 ed, Center for the Study of Language and Information, Stanford University, Stanford, 2006) http://plato.stanford.edu/archives/win2006/entries/privacy (accessed 26 February 2007); Brett Mason *Privacy without Principle: The Use and Abuse of Privacy in Australian Law and Public Policy* (Australian Scholarly Publishing, Melbourne, 2006) 52-80; Richard B Bruyer "Privacy: A Review and Critique of the Literature" (2006) 43 Alta L Rev 553; David Lindsay "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law" (2005) 29 Melb U LR 131; Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 125-133. Most of the articles cited in this section are reproduced in Raymond Wacks (ed) *Privacy* (2 vols, Dartmouth Publishing, Aldershot, 1993) and Eric Barendt (ed) *Privacy* (Dartmouth Publishing, Aldershot, 2001).

Reductionism

2.4 Reductionism is associated particularly with Judith Jarvis Thomson.[2] Thomson considers a number of scenarios that might be considered invasions of the right to privacy, but concludes in each case that they are in fact violations of some other right, such as the right over the person, the rights of property ownership, or the right to confidentiality. Thomson argues first that what is commonly described as the "right to privacy" is a cluster of rights, and that it is unclear what properly belongs in this cluster. Second, she argues that "there is no need to find the that-which-is-in-common to all rights in the right to privacy cluster and no need to settle disputes about its boundaries". This is because every right in the "right to privacy" cluster is also in some other cluster, and because the right to privacy is derivative in the sense that "it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning privacy".[3]

2.5 Thomson's reductionism has been criticised on two main grounds.[4] First, her argument relies on taking a very broad view of what is included in rights such as property rights and rights over the person. Her concept of "the right over the person" is particularly broad, and includes the right not to be looked at or listened to. Second, even if privacy rights are derivative, they may still form a coherent cluster. As Jeffrey Reiman notes:[5]

> [E]ven if privacy rights were a grab-bag of property and personal rights, it might still be revealing, as well as helpful, in the resolution of difficult moral conflicts to determine whether there is anything unique that this grab-bag protects that makes it worthy of distinction from the full field of property and personal rights.

The right to be let alone

2.6 The idea of privacy as "the right to be let alone" derives from a famous article on "The Right to Privacy" by Samuel Warren and Louis Brandeis,[6] and from Brandeis's equally famous dissent as a Justice of the United States Supreme Court in *Olmstead v United States*. Warren and Brandeis did not *define* privacy as "the right to be let alone", but they described recognition of the right to privacy as "the next step which must be taken for the protection of the person and for securing to the individual what Judge Cooley calls the right 'to be let alone'".[7]

2.7 In fact, the Warren and Brandeis article does not really provide either a definition or a coherent conception of privacy. It contains elements of a number of the other conceptions discussed below, including limited access to the self, control over personal information, and personhood. The principle on which the right to privacy rests, according to Warren and Brandeis, is that of "inviolate personality", the right to privacy being "part of the more general right to the immunity of the

2 Judith Jarvis Thomson "The Right to Privacy" (1975) 4 Philosophy and Public Affairs 295.

3 Ibid, 313.

4 Lindsay, above n 1, 145.

5 Jeffrey H Reiman "Privacy, Intimacy and Personhood" (1976) 6 Philosophy and Public Affairs 26.

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

7 Ibid, 195. Cooley had used this phrase in relation to attempted physical touching as a tort injury in his treatise on torts: Solove "Conceptualizing Privacy", above n 1, 1100.

person, – the right to one's personality".[8] The concept of "personality" was borrowed from the German legal and philosophical tradition.[9]

2.8 Privacy as the right to be let alone, or privacy as "non-interference",[10] assumed a more coherent form in two American jurisprudential streams that have flowed from the Warren and Brandeis article. First, there is the American tort of invasion of privacy, whose elements were set out in a 1960 article by William Prosser and subsequently adopted by the *Restatement of Torts*.[11] The four types of invasion of privacy identified by Prosser were, he said, tied together only by the fact that each represents an interference with the right to be let alone.[12] Second, there is the jurisprudence that finds a right to privacy in the United States Constitution. This is concerned with a more characteristically American conception of privacy, privacy as a protection for the citizen against intrusions by the state.

2.9 In "The Right to Privacy" Warren and Brandeis were concerned primarily with invasions of privacy by newspapers, but Brandeis's *Olmstead* dissent described the Constitution as conferring "*as against the Government*, the right to be let alone…. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[13] In 1967 Brandeis's view was adopted by the Supreme Court in *Katz v United States*,[14] overruling *Olmstead*, and thereafter privacy as the right to be let alone has frequently been invoked by the Court. Privacy has also been extended by the Court beyond Fourth Amendment search and seizure issues to matters such as rights to contraception and abortion.[15] The common theme in these decisions is one of privacy as a protection against intrusion or intervention by the state in private spaces or private matters.[16]

2.10 The main criticism of privacy as the right to be let alone is that it is simply too vague.[17] It leaves open the questions: in what ways, and in what matters, should we be let alone? As Anita Allen writes:[18]

> If privacy simply meant "being let alone", any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy. A punch in the nose would be a privacy invasion as much as a peep in the bedroom.

---

8 Warren and Brandeis, above n 6, 207.

9 James Q Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale LJ 1151, 1180-1185, 1206.

10 Bygrave, above n 1, 128.

11 William L Prosser "Privacy" (1960) 48 Cal L Rev 383. For more on the United States tort see New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) ch 4. For an explanation of the role of the Restatements of the Law, published by the American Law Institute, see ibid, 94, fn 13. The New South Wales Law Reform Commission cites the *Restatement (Second) of Torts*.

12 Prosser, above n 11, 389.

13 *Olmstead v United States* (1928) 277 US 438, 478 (Brandeis J, dissenting), quoted in Whitman, above n 9, 1213 (emphasis added).

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

15 Most notably in *Griswold v Connecticut* (1965) 381 US 479 (contraception); *Roe v Wade* (1973) 410 US 113 (abortion).

16 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) 671-678.

17 Solove "Conceptualizing Privacy", above n 1, 1101-1102.

18 Anita L Allen *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield, Totowa, NJ, 1988) 7.

In fact, even behaviour that is not offensive or harmful could be characterised as failing to let someone alone, and the only way of being truly let alone is to live in complete isolation from society. Moreover, the American jurisprudence that has come to associate the right to be let alone with non-interference by the state is of no assistance in understanding situations where state intervention to *protect* privacy against intrusions by other individuals or corporations may be called for.

Limited access to the self

2.11 Ruth Gavison has provided one of the most detailed formulations of the conception of privacy in terms of limited access to the self.[19] Gavison attempts to provide a "neutral" definition of privacy; that is, one that does not pre-judge which aspects of privacy are desirable or worthy of protection. Gavison defines privacy as "a limitation of others' access to an individual". In a state of perfect privacy (which Gavison acknowledges is impossible and generally undesirable in any society), a person would be completely inaccessible to others. She sees privacy as having three component elements. If X is in a state of perfect privacy, no one will have any information about X (secrecy), pay any attention to X (anonymity), or have physical access to X (solitude). The possession of privacy is not an all-or-nothing concept, however, and privacy can be lost to varying degrees as others gain information about, pay attention to, or gain physical access to a person.[20]

2.12 The main objection to Gavison's definition of privacy is that it is too broad: that treating *any* physical access to a person, or attention paid to a person, or information gained about a person as a loss of privacy robs privacy of much of its intuitive meaning.[21] Gavison and some other limited access theorists have been criticised for neglecting individuals' ability to choose to reveal aspects of themselves to others, and for failing to make clear what types of access implicate privacy.[22]

2.13 Nicole Moreham addresses these criticisms by including the element of "desire" in her definition of privacy as:[23]

> [T]he state of "desired 'inaccess'" or as "freedom from unwanted access". In other words, a person will be in a state of privacy if he or she is only seen, heard, touched or found out about if, and to the extent that, he or she wants to be seen, heard, touched or found out about. Something is therefore "private" if a person has a desire for privacy in relation to it: a place, event or activity will be "private" if a person wishes to be free from outside access when attending or undertaking it and information will be "private" if the person to whom it relates does not want people to know about it.

19 Ruth Gavison "Privacy and the Limits of the Law" (1980) 89 Yale LJ 421.

20 Ibid, 428. Gavison clarifies that physical access means "physical proximity – that Y is close enough to touch or observe X through normal use of his senses" (433).

21 Raymond Wacks *Personal Information: Privacy and the Law* (Oxford University Press, Oxford, 1993) 16-18.

22 Solove "Conceptualizing Privacy", above n 1, 1104.

23 N A Moreham "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 LQR 628, 636.

Thus, a person involuntarily stranded on a desert island is not experiencing privacy, nor does a person who willingly reveals something to another suffer an interference with privacy.[24] Desire acts as an important "limiting or controlling factor"[25] in Moreham's definition, but it could be considered that the factor introduced by Moreham is too individual and subjective.[26]

Concealment or control of personal information

2.14 Many theorists view privacy primarily or solely in terms of personal information. There are two main versions of this approach: privacy as *concealment or withholding* of information about the self, and privacy as *control* of such information.

2.15 A conception of privacy that equates it with the concealment of information about the self is found in Judge Richard Posner's economic critique of the right to privacy. While Posner deliberately avoids defining privacy, he notes that "one aspect of privacy is the withholding or concealment of information", and this is the aspect that he sees as particularly relevant to an economic analysis.[27] More particularly, Posner associates privacy with information that people will incur costs to conceal, particularly discreditable or embarrassing facts about themselves.[28] For Posner, privacy as concealment of discreditable information is a form of deception or manipulation, akin to "the efforts of sellers to conceal defects in their products".[29]

2.16 Wider critiques of Posner's economic analysis of privacy will not be considered here, but the conception of privacy as concealment of information about the self suffers from significant limitations. Solove argues that privacy "involves more than avoiding disclosure; it also involves the individual's ability to ensure that personal information is used for the purposes she desires".[30] In other words, privacy is not only about concealing or withholding information; it is also about being able to disclose information while retaining some control over the further dissemination of that information, or ensuring that the information is used only for particular purposes.

2.17 The conception of privacy as control over personal information is one of the more influential theories of privacy, and underlies data protection statutes in New Zealand and elsewhere that are labelled "Privacy" Acts. For example, Alan Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[31] (Westin's inclusion of information about groups or

24 Ibid, 636-637.

25 Wacks, above n 21, 18.

26 Moreham acknowledges the need for an "objective" check if her definition is to be employed in the legal context: Moreham, above n 23, 643-644.

27 Richard A Posner "The Right of Privacy" (1978) 12 Ga L Rev 393.

28 Ibid, 394; Richard A Posner *Overcoming Law* (Harvard University Press, Cambridge, Mass, 1995) 539; Richard A Posner *Economic Analysis of Law* (6 ed, Aspen Publishers, New York, 2003) 40.

29 Posner *Economic Analysis of Law*, above n 28, 40; Posner "The Right of Privacy", above n 27, 399-400.

30 Solove "Conceptualizing Privacy", above n 1, 1108.

31 Alan F Westin *Privacy and Freedom* (Atheneum, New York, 1967) 7. See Solove "Conceptualizing Privacy", above n 1, 1110, for other examples.

institutions in this definition is significant, but it is more common to limit such definitions to control of personal information by individuals.) Definitions of privacy in terms of control over personal information may acknowledge that the word "privacy" is not used only in relation to information, and that there are other aspects to privacy.[32] However, limiting privacy to control of personal information is a way of making the concept more coherent, and/or is seen as dealing with the central concerns that are most commonly raised in the name of privacy.[33]

2.18 The focus on *control* over personal information gets away from the problems of simply seeing privacy as concealment or withholding of information. It allows for the fact that privacy can also encompass individuals' interests in selective disclosure of personal information. Furthermore, once information has been disclosed, they may have a privacy interest in ensuring that personal information about them is used only for particular purposes, and that it is accurate.

2.19 However, control-based conceptions of privacy have also been criticised on a number of grounds. A particular variant of the conception of privacy as control over personal information sees personal information as the property of the person to whom it relates.[34] This presents problems because information is not like other commodities, as Solove points out:[35]

> Information can be easily transmitted, and once known by others, cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously in the minds of millions. This is why intellectual property law protects particular tangible expressions of ideas rather than the underlying ideas themselves. The complexity of personal information is that it is both an expression of the self as well as a set of facts, a historical record of one's behaviour…. Personal information is often formed in relationships with others, with all parties having some claim to that information.

2.20 Even if control of personal information is not equated with ownership, it still involves conceptual difficulties. Moreham identifies two such difficulties. First, it is possible for people to lose *control* over access to information about themselves without any such access actually being gained.[36] Second, it is difficult,

---

32 For example, immediately following the sentence quoted above, Alan Westin gives what appears to be a definition of another aspect of privacy: "Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve." Westin, above n 31, 7.

33 For example: Wacks, above n 21, 20-21, argues that privacy is not a useful or coherent term, but that the "central" or "archetypal" privacy concerns relate to the use, and especially the misuse, of personal information about an individual.

34 See for example Kenneth C Laudon "Markets and Privacy" (1996) 39 Communications of the ACM 92; Lawrence Lessig *Code and Other Laws of Cyberspace* (Basic Books, New York, 1999) 159-162; James Rule and Lawrence Hunter "Towards Property Rights in Personal Data" in Colin J Bennett and Rebecca Grant (eds) *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, Toronto, 1999) 168; Vera Bergelson "It's Personal But is it Mine? Toward Property Rights in Personal Information" (2003) 37 UC Davis L Rev 379. For critiques of this approach see Paul M Schwartz "Beyond Lessig's *Code* for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices" [2000] Wis L Rev 743; Jessica Litman "Information Privacy/Information Property" (2000) 52 Stan L Rev 1283.

35 Solove "Conceptualizing Privacy", above n 1, 1113.

36 Moreham gives the following example: "if an internet hacker, Y, had the technological ability to access and read all of X's personal emails then X would have lost control over access to information contained in them – and hence under a control definition, lost privacy – even if Y never actually broke into his account" (Moreham, above n 23, 638).

if not impossible, to truly control information. Moreover, disclosure of personal information is simultaneously an exercise and a relinquishment of control: A exercises control by disclosing personal information to B, but thereby loses control because B can now do what she likes with that information.[37] Moreham says that these conceptual problems can be avoided if control "is seen as a *means* of bringing privacy about rather than as privacy itself". In other words, control over information is a means of protecting privacy, but loss of control does not necessarily entail loss of privacy.[38]

2.21 Other criticisms relate to the focus on information, and apply equally to conceptions based on concealment and those based on control of personal information. It is suggested that the concept of "personal information" is just as vague and difficult to define as that of "privacy". Should all information about an individual be considered private, or only particular kinds of "sensitive" or "intimate" information? If the latter, how are we to know what is sensitive and intimate?[39]

2.22 Some writers also consider that the focus on information alone ignores other important privacy interests. In this view, there are significant invasions of privacy that do not involve, or do not principally involve, gaining information about people against their wishes. For example, most people would probably regard surveillance, spying and eavesdropping as invasions of privacy regardless of whether any new information, or any particularly sensitive information, is gained by these means.[40]

Personhood

2.23 Conceptions of privacy as personhood, like some conceptions that relate privacy to intimacy (see below), differ from the other theories discussed above in that they are concerned with the values that privacy protects, rather than with what privacy *is*. As such, they are often combined with other theories. We return to the question of privacy values in chapter 3.

2.24 As mentioned above, the concept of personality was central to the Warren and Brandeis article on "The Right to Privacy", and their use of the term appears to have been strongly influenced by German philosophy. In the German tradition personality (Persönlichkeit) was part of a concept of freedom "whose purpose was to allow each individual fully to realize his potential *as* an individual: to give full expression to his peculiar capacities and powers".[41] Conceptions of privacy as personhood, though not explicitly linked to this tradition, emphasise closely-related ideas of individuality, dignity and autonomy. For example, Stanley Benn grounds the general principle of respect for privacy in "respect for someone as a person, as a chooser, … as one engaged on a kind of self-creative enterprise, which could be disrupted, distorted or frustrated even by so limited an intrusion

37 Moreham, above n 23, 638.

38 Ibid, 639.

39 Solove "Conceptualizing Privacy", above n 1, 1111-1112; Moreham, above n 23, 642. For a discussion of this issue in relation to the Privacy Act 1993, see Paul Roth "What is 'Personal Information'?" (2002) 20 NZULR 40.

40 Moreham, above n 23, 649-651; Judith Wagner DeCew "The Scope of Privacy in Law and Ethics" (1986) 5 Law and Philosophy 145, 154-158.

41 Whitman, above n 9, 1181.

as watching".[42] Edward Bloustein picks up on Warren and Brandeis's concept of "inviolate personality", which he sees as "defining man's essence as a unique and self-determining being", and argues that the right to privacy is based on protection of individuality and human dignity.[43]

2.25 Benn and Bloustein are concerned primarily with privacy as a space in which individuals can develop free from public observation and public disclosure of their private lives. This is often spoken of in terms of autonomy, and is seen as essential to the functioning of democratic societies.[44] A stronger form of autonomy, the right of individuals to choose for themselves how to live their lives and to make decisions about certain matters free from state interference, is reflected in the United States "constitutional privacy" cases.[45] This version of privacy as personhood has been criticised on the grounds that it is really about liberty, not privacy. More generally, theories of privacy as personhood can be criticised for being too vague, and for using terms such as "individuality", "dignity" and "freedom" that are largely left undefined.[46]

Intimacy

2.26 The conception of privacy in terms of intimacy can be seen as a way of giving greater specificity to the personhood conceptions discussed above. A number of "privacy as intimacy" conceptions see privacy as creating the conditions for the development of intimate human relationships. For Charles Fried, who views privacy in terms of control over personal information:[47]

> [I]ntimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love.

Fried says that privacy also allows us to maintain degrees of intimacy with different people by disclosing differing amounts of information. However, this view has been criticised as simply defining intimate information as information that individuals choose to reveal selectively, without explaining what it is in the particular relationship that makes it intimate. For example, information might be revealed to a psychoanalyst that would never be told to a friend or lover, but this does not necessarily make the patient-psychoanalyst relationship an intimate one.[48]

2.27 Probably the most developed theory of privacy as intimacy, and one that provides a better explanation of the scope of intimacy, is that of Julie Inness. For Inness, intimate matters are those that draw "their value and meaning from the agent's love, care, or liking",[49] and privacy is:[50]

42 Stanley I Benn "Privacy, Freedom, and Respect for Persons" (1971) 13 Nomos 1, 26.

43 Edward J Bloustein "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 NYU L Rev 962, 971.

44 For example: Westin, above n 31, 33-34.

45 Levinson, above n 16, 671-675.

46 Solove "Conceptualizing Privacy", above n 1, 1118.

47 Charles Fried "Privacy" (1968) 77 Yale LJ 475, 484-485.

48 Reiman, above n 5, 33.

49 Julie C Inness *Privacy, Intimacy, and Isolation* (Oxford University Press, New York, 1992) 78.

50 Ibid, 91.

> [T]he state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring or liking. These decisions cover choices on the agent's part about access to herself, the dissemination of information about herself, and her actions.

Inness thus extends her definition of privacy beyond information. She also defines intimacy in terms of motives, not behaviours. This is because there is nothing about particular forms of behaviour in themselves that identifies them as intimate, and whether behaviours are considered intimate or not will vary across cultures and time periods.[51]

2.28 Conceptions of privacy as intimacy identify some important values that privacy protects and makes possible, and can assist in identifying a subset of "intimate" or "sensitive" personal information. Nevertheless, they have a number of flaws. Privacy may make it possible to develop feelings of trust, love, friendship and caring, but these ends do not form a complete picture of what is commonly considered to be protected by privacy. For example, financial information is usually considered private, but is often not regarded as intimate.[52] Inness contends that regulation of non-intimate personal information is more accurately described as secrecy, but she admits that this is a departure from common usage.[53]

2.29 Moreover, intimate and/or private matters need not be characterised by love or caring: sexual partners may feel no sense of caring for each other, and relationships between siblings or ex-spouses may be characterised by hatred yet still be considered private.[54] Inness acknowledges this, but argues that privacy should be extended over matters *commonly understood* as intimate until we have evidence that the actors involved are not in fact motivated by love, liking or care.[55] Privacy as intimacy also fails to account for those parts of private life that are focused on the self, rather than on relationships with others.[56]

2.30 Intimacy-based conceptions of privacy may also fail to capture many of the concerns about the building up of detailed personal profiles "through combining disparate pieces of ostensibly innocuous information", a process that is becoming ever easier with the increasing integration of information systems.[57]

2.31 Finally, in some circumstances intimacy, far from being facilitated by privacy, may "suffocate privacy".[58] This is particularly the case in small-scale societies where levels of intimacy may be high while levels of privacy are low. The relationship between privacy and intimacy posited by Inness and others appears to apply mainly in modern, individualist and predominantly urban societies.

---

51 Ibid, 74-77.

52 Solove "Conceptualizing Privacy", above n 1, 1123.

53 Inness, above n 49, 60-61.

54 Solove "Conceptualizing Privacy", above n 1, 1123-1124.

55 Inness, above n 49, 92.

56 Solove "Conceptualizing Privacy", above n 1, 1123-1124.

57 Bygrave, above n 1, 131.

58 Mason, above n 1, 69, citing David Flaherty *Privacy in Colonial New England* (University Press of Virginia, Charlottesville (VA), 1972).

Pragmatism

2.32 Having reviewed the conceptions of privacy outlined above, Daniel Solove sets out his own approach to privacy, which he describes as a pragmatic one. Solove proposes abandoning the search for a common denominator or essence of privacy. Instead, he suggests that privacy can usefully be conceptualised in terms of philosopher Ludwig Wittgenstein's notion of "family resemblances". Wittgenstein explained that certain concepts might not share one common characteristic, but might form "a complicated network of similarities overlapping and criss-crossing".[59] Where a traditional method of conceptualising might be likened to a wheel in which the spokes are all connected by the hub, an alternate method is to view concepts as webs made up of parts that are all connected but have no centre point. The boundaries of such concepts may be fuzzy or blurred, and/or constantly changing.[60]

2.33 Solove advocates a bottom-up rather than a top-down approach to conceptualising privacy: "We should act as cartographers, mapping out the terrain of privacy by examining specific problematic situations rather than trying to fit each situation into a rigid predefined category."[61] This approach to conceptualising privacy is context-specific, and involves examining privacy invasions as disruptions of particular practices. Such disruptions could include, for example, interference with peace of mind, intrusion on solitude, or loss of control over facts about oneself.[62] Solove notes that there are similarities and differences among both the disruptions and the practices they disrupt, and contends that "We should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted rather than looking for the common denominator that links all of them."[63]

2.34 Solove argues that the value of privacy is also context-specific, in contrast to theories that try to establish an overarching value of privacy such as protecting dignity or intimacy. For Solove, the value of privacy in particular contexts depends on the purposes of the practices involved, and the importance of those purposes. He also takes issue with theorists who argue that privacy has an intrinsic and inherently positive value, maintaining instead that it should be valued instrumentally, as a means to achieving other valuable ends.[64]

2.35 Solove suggests that "the landscape of privacy is constantly changing", particularly as a result of technological developments, and that scholars and judges may be led astray by trying to fit new problems into old conceptions.[65] Instead:[66]

> [W]e should seek to understand the special circumstances of a particular problem. What practices are being disrupted? In what ways does the disruption resemble or differ from other forms of disruption? How does this disruption affect society and social structure?

59 Ludwig Wittgenstein *Philosophical Investigations* (trans GEM Anscombe, 1958) §66, quoted in Solove "Conceptualizing Privacy", above n 1, 1097.

60 Solove "Conceptualizing Privacy", above n 1, 1098.

61 Ibid, 1126.

62 Ibid, 1129.

63 Ibid, 1130.

64 Ibid, 1143-1146.

65 Ibid, 1146.

66 Ibid, 1147.

2.36 Solove has applied this pragmatic approach in developing a taxonomy, or system of classification, of privacy, focusing on particular harms or problems.[67] However, he avoids the question of what it is that makes these problems of *privacy* rather than something else. He acknowledges that:[68]

> One might ask why we should even retain the term "privacy" if it is simply a broader way to describe a group of different types of harms. Why not simply refer to the particular harms themselves and jettison the term "privacy" altogether? But this view overlooks a key aspect of the way we refer to things and think about them. Although the various harms I identify in the taxonomy are different from one another, and although they do not have a core characteristic in common, they do … share many important similarities.

2.37 The main shortcoming of Solove's approach is that it provides no basis for establishing why some harms are privacy violations and others are not. To return to the words of Anita Allen quoted above, why is a peep in the bedroom an invasion of privacy but not a punch in the nose? However, a Wittgensteinian "family resemblances" approach to conceptualisation does not preclude attempts at definition. Solove notes that "We can draw fixed and sharp boundaries, but we do so for special purposes, not because the boundary is a necessary part of a conception."[69] One of those special purposes could be providing a definition for use in the law. Furthermore, a family resemblance concept can be explained "by a series of paradigmatic examples with the rider: 'and other similar things'".[70]

2.38 Another possible criticism of Solove's approach is that it is in fact a way of conceptualising privacy violations rather than privacy itself. His focus on harms in the form of disruption of specific practices lends itself well to a legal and policy analysis based on the prevention or remedying of harms, as we discuss further in chapter 3. However, while it is a useful way of understanding privacy violations or problems, it does not assist greatly in understanding what it means to experience privacy.

THE PRIVACY PARADIGM AND ITS CRITICS

2.39 Having set out some theories about how privacy should be conceptualised, we now identify some features of what Colin Bennett and Charles Raab have called the "privacy paradigm", and examine some critiques of that paradigm. Bennett and Raab use "paradigm" to mean:[71]

> a set of assumptions about a phenomenon or area of study that generally go unquestioned. These assumptions collectively set the agenda for research and for policy prescription. The paradigm produces an agreed understanding about the nature and scope of a particular problem.

67 Daniel Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477.

68 Ibid, 562, fn 480.

69 Solove "Conceptualizing Privacy", above n 1, 1098.

70 Peter Hacker "Family Resemblance" in Ted Honderich (ed) *The Oxford Companion to Philosophy* (Oxford University Press, Oxford, 1995) 269.

71 Colin J Bennett and Charles D Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge, Mass, 2006) 4. Bennett and Raab identify assumptions and implications of the privacy paradigm at pages 4-11. Our analysis of the privacy paradigm draws on theirs, although it does not follow it exactly.

The privacy paradigm, then, consists of a set of assumptions that underlie much of the legal and policy framework and analysis of privacy protection in Western societies such as New Zealand. Some features of the privacy paradigm may seem obvious, but because they are usually unexamined it is worth making them explicit. As we shall go on to show, these assumptions have been challenged by critics from a variety of perspectives.

Assumptions of the privacy paradigm

2.40 A key assumption of the privacy paradigm is some idea of a public/private divide. The public/private distinction has a long history in Western cultures, and is the subject of an extensive literature, which it is not possible to review here.[72] The concept of distinct public and private spheres is central to modern liberalism, and is reflected in the division of law into public law (which concerns the relationship between individuals and the state) and private law (which concerns the relationships between individuals). However, like "privacy", the terms "public" and "private" are used in a number of different senses. Ruth Gavison identifies three important senses of the distinction:[73]

- *Accessible/inaccessible*. The private is that which is not observed or known by people generally, or whose use or enjoyment is restricted to particular people; the public is that which is open to people generally, and/or can readily be known or observed by people generally.
- *Freedom/interference*. The private is the sphere in which others do not interfere; the public is the sphere governed by some degree of regulation or prohibition (whether by the state or by social convention).
- *Individuals/society (groups)*. The public/private distinction can be used to distinguish between matters pertaining to individuals or groups and those that concern larger social entities. Beate Rössler explains this in terms of an onion model, with the individual at the centre contrasted with the outer public layers; then the family, which is private in comparison with the wider society; then the domain of groupings such as private businesses and civil society, which are still private in relation to the state; and finally, the outer layer of the state, which is public in relation to all the other layers.[74]

2.41 Gavison points out that these different meanings can be combined to create more complex clusters of meaning, and that further complexities are introduced when descriptive senses are distinguished from normative ones (what is in fact observed by others versus what *should be* observed by others, for example). Further, the different senses are distinct and yet interrelated.[75] It is notable that the home and the family, commonly seen as the paradigmatic example of the private sphere in modern Western societies, generally fall within the meaning of "the private" in each of the three senses identified by Gavison. While the meanings of "public" and "private" are complex and at times ambiguous, some sense of this distinction is central to the privacy paradigm.

72 For some brief overviews see Wacks, above n 21, 7-9; Mason, above n 1, 9-28; Graeme Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (Cambridge University Press, Cambridge, 2002) 28-32; Ruth Gavison "Feminism and the Public/Private Distinction" (1992) 45 Stan L Rev 1, 4-10; Hannah Arendt *The Human Condition* (2 ed, University of Chicago Press, Chicago, 1958) 22-78.

73 Gavison "Feminism and the Public/Private Distinction", above n 72, 6-7.

74 Beate Rössler "Privacies: An Overview" in Beate Rössler (ed) *Privacies: Philosophical Evaluations* (Stanford University Press, Stanford, 2004) 1, 6.

75 Gavison "Feminism and the Public/Private Distinction", above n 72, 7-10.

2.42 Some further assumptions of the privacy paradigm are that certain matters (such as access to personal information) should be understood primarily in terms of protection of privacy, rather than other values; that it is important to protect privacy; and that privacy is under threat in contemporary society.

2.43 The privacy paradigm's assumption that it is important to protect privacy is based on the belief that some level of privacy is a basic human need and, more particularly, that privacy is essential to the functioning of liberal democratic societies.[76] The privacy paradigm conceives of society as made up of autonomous individuals who require a sphere of privacy in order to carry out their various roles as citizens of a liberal democratic state.[77] Privacy is thus generally seen as an individual right or claim, and privacy protection is justified primarily in individualistic terms, although its wider social benefits may also be recognised.[78]

Critiques of the privacy paradigm

2.44 The assumptions of the privacy paradigm have been criticised from a range of perspectives. One critique is that privacy is simply too conceptually incoherent to be useful, and that this conceptual incoherence gives rise to incoherent law and policy.[79] We will set out our own views on conceptualising privacy in a way that may usefully inform law and policy in the chapter that follows. We also reserve for consideration in chapter 5 the question of the extent to which the privacy paradigm is the product of a particular culture and history. We discuss here a number of other critiques which, while not invalidating the privacy paradigm, stand as important counterpoints to it. We also consider responses to these critiques.

Feminism and the public/private distinction

2.45 Critique of the public/private distinction can be found in writing that has emerged from the critical legal studies movement in the United States and is central to the work of many feminist theorists.[80] Indeed, Carole Pateman has argued that the public/private dichotomy "is, ultimately, what the feminist

76 See for example Westin, above n 31, chs 1-2.

77 Bennett and Raab, above n 71, 4-5.

78 Ibid, 6-7.

79 This is the argument of Mason, above n 1.

80 See Anita Allen "Privacy in American Law" in Beate Rössler (ed) *Privacies: Philosophical Evaluations* (Stanford University Press, Stanford, 2004) 19, 34, for a summary of "left progressive" critiques from critical legal studies.

movement is about".[81] At the risk of oversimplifying and of playing down differences between feminist theorists, the core of the feminist critique of the public/private distinction (and, by extension, of privacy) is as follows:

- The public sphere has been seen as the privileged, male sphere of power, from which women have been systematically excluded, while the private sphere of domestic life has been devalued and constrained because it has been seen as "women's realm".
- Even within the private sphere, women have had little or no autonomy, and have been subject to male domination. "Privacy" has acted as a shield for male power in the private sphere, creating a space in which men are presumed to be unaccountable for their actions and free from state intervention that might help to overcome power inequalities.

2.46 Feminist critiques of privacy and the public/private distinction provide important insights into the ways in which these concepts have acted to entrench male power and privilege. A number of feminist theorists have pointed out, however, that it does not follow that the ideas of privacy and the private sphere are inherently oppressive for women, or that feminists should reject privacy outright. Writers such as Anita Allen have argued that, while feminists should continue pointing out the socially-constructed nature of the public/private divide and the need to renegotiate this boundary in the interests of promoting dignity and equality, women as much as men need the space for "solitude, independent reflection, true intimacy, and moral choice" that privacy provides.[82] Indeed, while privacy's most trenchant feminist critic, Catharine MacKinnon, may write that feminism "has had to explode the private",[83] it is questionable whether any feminist critic really advocates the complete abolition of all distinction between the public and the private.[84] It should also be borne in mind that much of the feminist critique of privacy comes from the United States, and is focused on whether the framing of Supreme Court decisions on sexuality and reproductive choice in terms of decisional privacy is positive or negative for women. Such debates have less relevance for the questions of informational and spatial privacy with which we are concerned in this study paper.

---

81 Carole Pateman "Feminist Critiques of the Public/Private Dichotomy" in SI Benn and GF Gaus (eds) *Public and Private in Social Life* (1983) 281, quoted in Gavison "Feminism and the Public/Private Distinction", above n 72, 1 (n3). The feminist literature on the public/private distinction and privacy is vast. In addition to the article by Ruth Gavison, relevant works include Allen *Uneasy Access*, above n 18; other work by Anita Allen cited in Anita L Allen *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability* (Rowan & Littlefield, Lanham, Maryland, 2003) 12-13 (n 17); Judith Wagner DeCew *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Cornell University Press, Ithaca, 1997) 81-94; Elizabeth M Schneider "The Violence of Privacy" (1991) 23 Conn L Rev 973 and also published in revised form in Elizabeth Schneider *Battered Women & Feminist Lawmaking* (Yale University Press, New Haven, 2000) 87-97; Tracey E Higgins "Reviving the Public/Private Distinction in Feminist Theorizing" (2000) 75 Chi-Kent L Rev 847; Annabelle Lever "Must Privacy and Sexual Equality Conflict? A Philosophical Examination of Some Legal Evidence" (2000) 67 Social Research 1137; Beate Rössler "Gender and Privacy: A Critique of the Liberal Tradition" in Beate Rössler (ed) *Privacies: Philosophical Evaluations* (Stanford University Press, Stanford, 2004) 52.

82 Allen "Privacy in American Law", above n 80, 35-36.

83 Catharine A MacKinnon *Toward a Feminist Theory of the State* (1989) 191, quoted in Gavison "Feminism and the Public/Private Distinction", above n 72, 2.

84 Gavison "Feminism and the Public/Private Distinction", above n 72, 28-29.

Anti-social privacy?

2.47 As long ago as 1949, economist Heinz Arndt criticised what he called "the cult of privacy" for protecting anti-social behaviour and promoting a conception of society based on selfish individualism.[85] More recently, utilitarian legal academic Mirko Bagaric has claimed that "privacy is destructive of our wellbeing. It prevents us attaining things that really matter, such as safety and security and makes us fear one another".[86] The most extended critique of privacy for its perceived privileging of individualism over the common good has come from sociologist and communitarian Amitai Etzioni. Focusing on the contemporary United States, Etzioni argues that privacy has come to be treated as a highly privileged value, rather than as something to be balanced against social responsibilities and concerns for the common good. According to Etzioni, excessive privacy demands have had "significant and detrimental effects" in a number of areas of public policy.[87]

2.48 Etzioni does not argue, however, that privacy is unimportant or should not be protected; on the contrary, he believes that "without privacy no society can long remain free".[88] He simply considers that the pendulum has swung too far in the direction of privacy, and that balance needs to be restored by treating privacy "as one good among others, without a priori privileging any of them".[89] In addition, while it is true that privacy is often justified in individualist terms, there are social or "common good" grounds for protecting privacy as well.[90] These include arguments that privacy protects aspects of freedom of speech and association that are essential to the functioning of democratic societies, and provides the conditions for a healthy public sphere by allowing individuals to keep private some things that might divide them and to operate on the basis of commonalities.[91] Likewise, protecting the privacy of health records ensures that individuals are able to talk freely to their doctors about their health problems, which in turn helps to protect the wider society from the spread of disease.[92] The work that relates privacy to the development of intimate relationships, discussed above, also helps to answer the criticism that privacy is selfish, isolating or anti-social.

---

85 H Arndt "The Cult of Privacy" (1949) 21 Australian Quarterly 69-71, quoted in Bennett and Raab, above n 71, 14.

86 Mirko Bagaric "Privacy is the Last Thing we Need" (22 April 2007) *The Age* Melbourne www.theage.com.au (accessed 23 April 2007). See also Philip Leith "The Socio-Legal Context of Privacy" (2006) 2 International Journal of Law in Context 105, 106: the individualistic approach to privacy "leads us to attempt the development of a pathological society – in a Durkheimian sense – in which social benefit is forever playing second fiddle to individual desire".

87 Amitai Etzioni *The Limits of Privacy* (Basic Books, New York, 1999) 7.

88 Ibid, 1.

89 Ibid, 4.

90 The social value of privacy is explored in Priscilla M Regan *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, Chapel Hill, 1995) ch 8; Priscilla M Regan "Privacy as a Common Good in the Digital World" (2002) 5 Information, Communication and Society 382. See also Ferdinand David Schoeman *Privacy and Social Freedom* (Cambridge University Press, Cambridge, 1992).

91 Bennett and Raab, above n 71, 41. On the latter point see also Thomas Nagel "Concealment and Exposure" (1998) 27 Philosophy and Public Affairs 3, reproduced at www.nyu.edu/gsas/dept/philo/faculty/nagel/papers/exposure.html (accessed 29 January 2007); Jeffrey Rosen *The Unwanted Gaze: The Destruction of Privacy in America* (Random House, New York, 2000).

92 It is notable that privacy of medical records is one area in which Amitai Etzioni thinks *more* privacy protection is needed: Etzioni, above n 87, ch 5.

Privacy as deception

2.49 We have referred above to Judge Richard Posner's view that privacy is essentially a form of fraud or deception; that it protects individuals who seek to conceal facts about themselves that others have an interest in knowing, and prevents others from obtaining information that might prove or disprove the claims that people make about themselves.[93] Posner objects to this on grounds of economic efficiency, but there are also other reasons for arguing that people should not have a legal right to conceal information about themselves in the name of privacy.[94] Mirko Bagaric claims that a strong right to privacy "is no more than a request for secrecy – refuge of the guilty, paranoid and misguided",[95] and the argument that "if you have nothing to hide, you have nothing to fear" is sometimes raised against privacy.[96] Privacy may also be seen as a form of licensed hypocrisy, allowing people to lead one life in public and an entirely different, and perhaps quite inconsistent, one in private.

2.50 One response to this critique is that, by focusing on concealment of information about the self, it takes an overly-narrow view of privacy. It is also argued that it is based on a simplistic understanding of human personality and social interaction.[97] The idea that a person's public "face" is simply a mask for their real, private self is seen as misleading, since personality is not unitary and people wear different "masks" in different contexts. All of these personas are equally true, or equally part of an individual's personality. Far from privacy being a licence for hypocrisy, the *decline* of privacy can be seen as encouraging hypocrisy, since people may become more careful even in private to express only socially-approved views, or to behave only in socially-approved ways, regardless of their actual opinions or desires. Moreover, tearing away a person's public masks by revealing aspects of his or her private life can be seen as profoundly wounding, leaving the individual exposed and vulnerable. It seems probable that all of us have "something to hide" from the world at large (perhaps even from those with whom we are intimate), and that these "somethings" need not be truly reprehensible for us to want to keep them private.

2.51 Nevertheless, there is a real tension between the virtues of transparency and openness and those of privacy and reticence. We will discuss this tension further in chapter 8, and in later reports for this Review. A key question for law reform is the extent to which the law should intervene in the "informational dance" between individuals trying to present a particular image of themselves and others trying to test that image against additional information.[98]

---

93 Posner "The Right of Privacy", above n 27, 399-400.

94 Philip Leith argues in very similar terms to Posner, but bases his argument on the sociological theories of Erving Goffman: Leith, above n 86, 109-112.

95 Bagaric, above n 86.

96 As Paul Chadwick notes, the implication of this phrase is that "only the guilty, with shameful secrets, object to having details of their lives known": Paul Chadwick "The Value of Privacy" (2006) 5 EHRLR 495, 504. For further discussion see Daniel J Solove *"I've got Nothing to Hide" and other Misunderstandings of Privacy* (George Washington University Law School Public Law Research Paper no 289, 2007).

97 Nagel, above n 91; Rosen, above n 91, 210; Daniel J Solove *The Future of Reputation: Gossip, Rumour, and Privacy on the Internet* (Yale University Press, New Haven, 2007) 68-70. Both Rosen and Leith (cited above) make extensive use of the work of Erving Goffman, but to different ends: see Erving Goffman *The Presentation of Self in Everyday Life* (Allen Lane The Penguin Press, London, 1969 [originally published 1959]).

98 Leith, above n 86, 109, 112.

2.52 Some writers on matters that are commonly considered in terms of privacy maintain that analysis from within the privacy paradigm gives insufficient attention to questions of power and the reinforcement of inequality.[99] This critique can be found particularly in the field of "surveillance studies" that has developed separately from privacy studies, but examines some of the same issues.[100] At its most pessimistic, surveillance studies can exhibit a type of fatalism, with surveillance being seen as so embedded in the institutions, systems and practices of modern life that it cannot be resisted.[101] More commonly, however, surveillance studies sees surveillance as something that can be controlled, but not by privacy-protection measures alone. An exclusive focus on privacy is said to overlook the increasing use of surveillance for "social sorting": the exercise of social control through the categorisation of individuals on the basis of certain characteristics. Examples can include identifying people from particular ethnic or religious backgrounds for greater scrutiny as potential terrorists, or charging different prices for the same goods on the basis of the buyers' perceived ability to pay. Social sorting can be seen as arbitrary (in that people can be identified for special treatment without good cause) and at the same time discriminatory (in that people can be selected for special treatment, whether good or bad, on the basis of characteristics over which they have no control). It is therefore seen as potentially reinforcing existing inequalities and/or creating new ones.[102]

2.53 Except in its most pessimistic form, surveillance studies complements, rather than contradicts, privacy-centred analysis. The "popular cachet" of privacy can, however, be an obstacle to explaining why privacy is not the only problem posed by surveillance, in the view of David Lyon.[103] According to Lyon, "large and urgent questions about social sorting remain, even after privacy and data protection policies and laws have done their work."[104] The Surveillance Studies Network suggests that privacy protection "might be the first line of defence against the undesirable effects of surveillance", but could be viewed as

99 Rosa Ehrenreich "Privacy and Power" (2001) 89 Geo L J 2047.

100 See Bennett and Raab, above n 71, 18-22; David Lyon "Surveillance, Power and Everyday Life" in Robin Mansell, Chrisanthi Avgerou, Danny Quah and Roger Silverstone (eds) *The Oxford Handbook of Information and Communication Technologies* (Oxford University Press, Oxford, 2007) 449; Martin Hirst and John Harrison *Communication and New Media: From Broadcast to Narrowcast* (Oxford University Press, South Melbourne, 2007) chs 13-14; Felicity Brown "Rethinking the Role of Surveillance Studies in the Critical Political Economy of Communication" (paper for the International Association for Media and Communication Research conference, Cairo, Egypt, 23-28 July 2006); Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006); Clive Norris and Dean Wilson (eds) *Surveillance, Crime and Social Control* (Ashgate Publishing, Aldershot, 2006); the website of the Surveillance Project, Queens University, Kingston, Ontario, Canada www.queensu.ca/sociology/Surveillance; and the online journal *Surveillance & Society* www.surveillance-and-society.org.

101 Perri 6 *The Future of Privacy* (vol 1, Demos, London, 1998) 55; Brown, above n 100, 3-7. This view is associated particularly with certain interpretations of the work of French philosopher Michel Foucault.

102 For further discussion of social sorting see Surveillance Studies Network, above n 100, especially 6-8, 30-33, 43-45; David Lyon (ed) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge, Abingdon, 2003).

103 Lyon "Surveillance, Power and Everyday Life", above n 100, 449, 460.

104 Ibid, 465.

insufficient on its own to deal with these effects. They conclude, however, that "surveillance protection is highly likely to coincide with, and to borrow from, the experience and infrastructures of privacy or data protection."[105]

PRIVACY AND OTHER CONCEPTS

2.54 Privacy is closely related to, overlaps with, and is sometimes confused with certain other concepts. We consider in this section how privacy may be distinguished from secrecy, confidentiality, reputation and property. In doing so we take account of the meanings that some of these terms have acquired in law, but do not attempt here to provide a comprehensive legal analysis.

Secrecy

2.55 A secret can be defined as something (especially information) that is intentionally withheld or kept hidden by one or more social actor(s) from one or more other social actor(s), and secrecy refers to the methods and practices of such concealment.[106] Some conceptions of privacy (such as Gavison's) see secrecy as an aspect of privacy, and the two concepts clearly overlap. There are, however, a number of ways in which the two concepts can be distinguished:

- Privacy is generally seen as applying only to individuals (although there is an argument for applying it to groups, which we will consider elsewhere). By contrast, groups, organisations and governments can have secrets and maintain secrecy.
- As a consequence of the first point, secrecy need not relate to personal information: there can be military secrets or trade secrets, for example, that do not include information about particular individuals.
- Secrecy does not necessarily protect information because of its private or intimate nature. Secrets may be kept for a wide range of reasons: for example, because the information could be dangerous, or could be used by others to their own advantage, if revealed more widely.
- Secrecy tends to convey a stronger sense of boundaries, and of being either on the inside or the outside, than privacy. A secret is generally seen as something that should not be divulged, except under specific conditions or circumstances, whereas a private matter is something that the person to whom it relates may choose to disclose.[107]

2.56 Secrecy and privacy are often confused because secrecy *can* protect privacy, either intentionally or as a by-product of protecting other interests. For example, the secrecy provisions of the Tax Administration Act 1994 are primarily intended to protect "the integrity of the tax system" and the government's ability

105 Surveillance Studies Network, above n 100, 76. For a view that is more sceptical of the value of privacy in addressing problems of surveillance see Felix Stalder "Privacy is not the Antidote to Surveillance" (2002) 1 Surveillance & Society 120.

106 Kim Lane Scheppele *Legal Secrets: Equality and Efficiency in the Common Law* (University of Chicago Press, Chicago, 1988) 12-16; Sissela Bok *Secrets: On the Ethics of Concealment and Revelation* (Pantheon Books, New York, 1982) 5-7. Bok notes that things as well as information can be secret, but even in such cases keeping the secret means withholding information about the existence or nature of the thing.

107 According to Edward Shils: "In secrecy, disclosure or acquisition beyond the boundary is prohibited, and the prohibition is attended by sanctions in event of a breach. In privacy, disclosure is at the discretion of the possessor, and such sanctions as laws provide are directed only against coercive acquisition by persons outside the boundary." Edward Shils "Privacy: Its Constitution and Vicissitudes" (1966) 31 Law & Contemp Probs 281, 283 (n 1).

to gather revenue through taxes.[108] However, these provisions also act as a strong protection against disclosure of the private financial and other information of individuals. At the same time, if privacy is conceived of in terms of control by individuals over their personal information, privacy and secrecy can sometimes conflict. If individual taxpayers want access to information about themselves held by the Inland Revenue Department (for example, to check its accuracy), such access may be denied on the grounds of secrecy.[109]

Confidentiality

2.57 Confidentiality is closely related both to secrecy and to privacy.[110] It is generally concerned with relationships in which one party has entrusted information to the other on the understanding that it will not be disclosed further.[111] For example, patients tell information to their doctors on the understanding that medical confidentiality protects them from having that information disclosed further (except with their consent or within certain strict limits). Confidentiality is related to secrecy because it concerns shared secrets, and to privacy because often the confidential information will also be private in nature. However, confidentiality is concerned with the circumstances in which the information was acquired, while privacy is concerned with particular types of information (private or personal information). Imagine that A knows private information about C and tells it in confidence to B, then B publishes that information. Both A and B may have breached C's privacy, but it is A whose confidence has been breached.

Reputation

2.58 The close relationship between privacy and reputation is apparent in the fact that the right to privacy and the right to protection against attacks on honour and reputation appear in the same articles of the Universal Declaration of Human Rights (article 12) and the International Covenant on Civil and Political Rights (article 17). The association is particularly strong in European civil law, where privacy law has a strong emphasis on protecting honour and on control by individuals over their public image.[112] Reputation is concerned with a person's

108 Tax Administration Act 1994, s 6 refers to protecting the integrity of the tax system; note that this includes protecting the confidentiality of the affairs of taxpayer (s 6(2)(c) and (e)). Sections 81, 86 and 87 deal with requirements to maintain secrecy. A recent case discussing the intersection between the Privacy Act 1993 and the secrecy provisions of the Tax Administration Act is *Forrest v Inland Revenue Department* (5 October 2007) Human Rights Review Tribunal 19/07.

109 For discussion of the relationship between privacy and official regimes of secrecy see Australian Law Reform Commission *Privacy* (vol 1, ALRC 22, Australian Government Publishing Service, Canberra, 1983) 27-28; Australian Law Reform Commission *Review of Australian Privacy Law* (ALRC DP72, Sydney, 2007) 476-481.

110 Law Commission *Breach of Confidence* (Law Com 110, HMSO, London, 1981) 5-7; Australian Law Reform Commission *Privacy*, above n 109, 28-29; Bok, above n 106, 119; Laurie, above n 72, 211-218; John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, South Melbourne, 2005) 203-233, especially 230; Neil M Richards and Daniel J Solove "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Geo LJ 123.

111 However, the concept has been extended further in the English courts: Burrows and Cheer, above n 110, 213-215.

112 For a historical account of the development of this emphasis in French and German law see Whitman, above n 9, 1164-1195.

standing in the eyes of others.[113] It is one of the interests that can be protected by privacy law, and it is also protected by defamation law, with the distinction generally being that defamation protects against falsehoods that may lower a person's reputation while privacy protects against the release of true information about a person's private life that may adversely affect the individual's reputation. However, privacy protection often extends well beyond information that might damage reputation, as the Australian Law Reform Commission points out:[114]

> Privacy interests might be affected by material about an individual which is perfectly true and neutral but which he simply does not want others to know, for example, personal tastes, address, income or age.... [C]laims to "information privacy" have arisen not so much out of a concern in the individual to control the flow of untrue and disparaging information about him, but more from a desire to see that true information, indeed the information that he might himself have divulged to the record keeper, is kept secure and is treated fairly.

Property

2.59 Property is perhaps the most complex of all the concepts that need to be disentangled from privacy.[115] Legal protection of private property plays an important role in protecting privacy,[116] although, as we discuss further in chapter 4, the privacy dimension of property rights was not necessarily made explicit in earlier times. One of the most original aspects of Warren and Brandeis's "Right to Privacy" was their attempt to cut privacy loose from property and establish it as a distinct right based on the principle of "inviolate personality".[117] This attempt was only partly successful, however, and very quickly the right to privacy as recognised in United States courts "began to develop distinctly proprietary attributes".[118] There is also a school of thought that advocates protecting informational privacy by creating a property right in personal information.[119] In the area of bodily privacy, too, there are competing conceptions of control over and autonomy in one's body in terms of privacy and property rights.[120]

---

113 Reputation is discussed further in Solove "A Taxonomy of Privacy", above n 67, 551; Huw Beverley-Smith *The Commercial Appropriation of Personality* (Cambridge University Press, Cambridge, 2002) 249-270, especially 250-252.

114 Australian Law Reform Commission *Privacy*, above n 109, 30.

115 We do not intend here to define property, or to enter into the debate about how it should be defined.

116 Jeremy Waldron *The Right to Private Property* (Oxford University Press, Oxford, 1988) 295-296.

117 Warren and Brandeis, above n 6, especially their discussion of the legal protection of personal writings and artistic productions at 200-205.

118 Beverley-Smith, above n 113, 156. There developed within the United States privacy tort a right to protection against commercial or other appropriation of name or likeness, and this further evolved in some states into a "right of publicity" protecting celebrities' right to exclusive use of their name and likeness. The former could protect both dignitary and property interests, while the latter is more clearly based on a property right. See generally Beverley-Smith's book just cited; New South Wales Law Reform Commission *Invasion of Privacy* above n 11, 111-115; Robert C Post "Rereading Warren and Brandeis: Privacy, Property and Appropriation" (1991) 41 Case West Reserv Law Rev 657, 670-680.

119 See references at n 34 above. A useful recent review of the debate over this idea is Corien Prins "When Personal Data, Behaviour and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?" (2006) 3 SCRIPT-ed 270.

120 Laurie, above n 72, 299-328; Radhika Rao "Property, Privacy, and the Human Body" (2000) 80 BUL Rev 359. Rao is concerned mainly with the United States doctrine of constitutional privacy, which protects decision-making by individuals in relation to their bodies and intimate relationships.

2.60 Privacy has been unable to completely shake off its connection with property because there are strong affinities between the two concepts, as well as significant differences. The extent of these affinities and differences depends on how both privacy and property are conceptualised. As we have mentioned, property rights can protect privacy, particularly in the home. Radhika Rao points out that both privacy and property draw on territorial metaphors, using images of bounded spaces and protected spheres surrounding the individual. Both concepts also involve some sort of right to exclude unwanted interference or intrusion by others.[121]

2.61 Some key differences between property and privacy are that:[122]

- Property is normally alienable, and can be sold, assigned or otherwise transferred to others; privacy cannot. As Rao puts it:[123]

  > [T]o the extent that privacy represents a principle of personal autonomy, it is a right that by its very nature is inseparable from the individual and incapable of being exercised by another. Accordingly, the idea that one individual may exercise another's privacy right is incoherent.

  It may be the case that a person's privacy can be given up in exchange for payment,[124] or that one person can lay a complaint about interference with another person's privacy,[125] but neither of these situations involve the *transfer* of one person's privacy right or interest to another.
- Property rights can survive the owner's death; privacy rights are often considered to cease on the individual's death (although, as we discuss further in chapter 8, this is by no means clear either legally or morally).
- Inequality goes hand in hand with private property in the sense that some people may own much while others own little; significant inequalities in the distribution or protection of privacy are generally considered undesirable.
- Property allows for aspects of personality (such as images or pieces of personal data) to be detached from the individual and commodified; privacy is based on a conception of personality as being intrinsically attached to the identity of a particular, usually living, individual.

121 Rao, above n 120, 418-428.

122 Post, above n 118, 663-670; Rao, above n 120, 428-443.

123 Rao, above n 120, 437. There are forms of inalienable property, but alienability is the norm.

124 For example, in *Douglas v Hello! Ltd* [2001] QB 967, 1006, Sedley LJ said that the celebrity claimants had "sold most of the privacy they now seek to protect … for a handsome sum" in selling exclusive rights to photographs of their wedding to a particular magazine.

125 This is the case, for example, in the privacy jurisdiction of the Broadcasting Standards Authority under the Broadcasting Act 1989. In consultations about the BSA's privacy principles, broadcasters argued that only people personally affected by an alleged breach of privacy should be able to complain, while children's advocates supported the opportunity to bring third-party complaints: Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press/ Broadcasting Standards Authority, Wellington, 2004) 62. The High Court confirmed in *TV3 Network Services Ltd v ECPAT New Zealand Inc* [2003] NZAR 501, 505 (HC) Chambers J, that any person may complain under the Broadcasting Act 1989 about a breach of broadcasting standards in relation to privacy, not only the person whose privacy is directly affected.

CONCLUSION

2.62 Our exploration of different theories of privacy in this chapter suggests to us that no one theory on its own has yet captured all the complexities of privacy. We strongly suspect that any attempt to provide a comprehensive definition of privacy is doomed to failure, and we will not seek to provide such a definition in this study paper. That does not mean, however, that we consider the concept of privacy to be meaningless. We have shown in this chapter, for example, that it can be usefully distinguished from certain related concepts. Nor do we believe that privacy is incapable or unworthy of legal protection. While there is much validity in critiques of the privacy paradigm, each of these critiques has its own shortcomings. We set out our own conceptual approach to privacy, and the basis for what should be protected, in the next chapter.

Chapter 3:

A Conceptual Approach to Privacy

3.1 The previous chapter discussed theories of privacy that have been developed in the international literature. The range and variety of these approaches has given rise to the impression in some quarters that the concept of "privacy" is incomplete and unsatisfactory. Indeed, it has become almost axiomatic to say that privacy is a "notoriously elastic concept",[1] that it has a "protean capacity to be all things to all lawyers",[2] that it is "infected with pernicious ambiguities",[3] or that there are "few concepts more vague or less amenable to definition".[4] Some authors have therefore resisted the attempt to pursue definition, saying that the imprecision of the concept means that it is of little assistance in developing law and policy. It is better, some say, to simply describe the garden varieties of dimensions or attributes of what might be called "privacy". On this view, examples of privacy and invasions of it, rather than what might be seen as an elusive core concept, drive description and analysis.

3.2 Our objective in this chapter is to set out a conceptual approach to privacy that we believe will assist the Commission in developing proposals for law and policy in the course of this Review.[5] Our intention is not to develop a definitive conceptual approach to privacy. Rather, the approach is intended to assist analysis and to invite discussion that might ultimately lead the Commission to adjust the assumptions underlying the conceptual framework or to particularise them further.

3.3 In this chapter, we are principally concerned with exploring what dimensions or interests ought to be considered as constituting the concept of "privacy". We are also concerned with whether the right to, or interest in, privacy is one that the law should intervene to protect. Some aspects of privacy may be better left as non-justiciable. Others may already be protected by a range of areas of law that are not explicitly grounded in privacy values.

1 Anita Allen *Uneasy Access: Privacy for Women in a Free Society* (Random and Littlefield, Totowa, 1988) 16.

2 T Gerety "Redefining Privacy" (1977) 12 Harv CR-CLL Rev 233, 234.

3 Hyman Gross "The Concept of Privacy" (1967) 42 NYULR 34, 53.

4 Robert G Dixon "The *Griswold* Penumbra: Constitutional Charter for an Expanded Right of Privacy?"(1965) 64 Mich L Rev 197, 199.

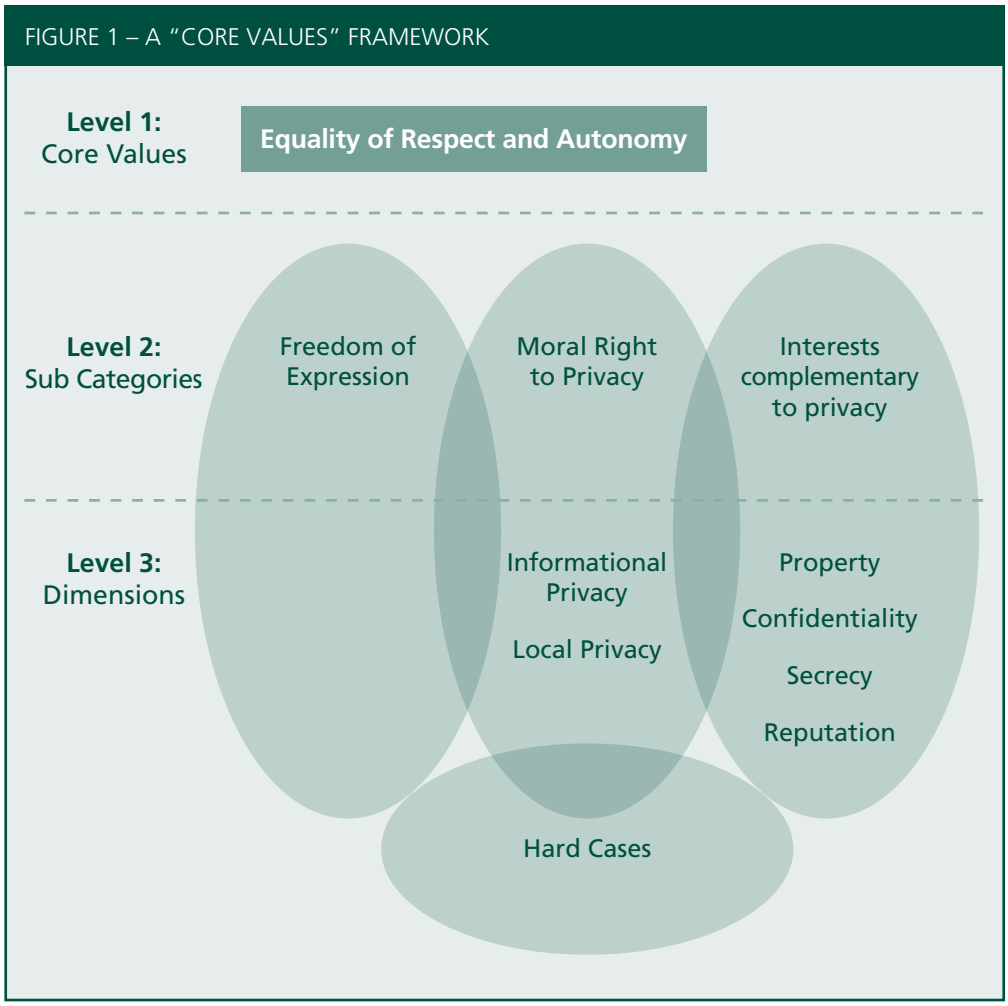
5 This chapter is based in part on Mark Hickford *A Conceptual Approach to Privacy* (NZLC MP19, Wellington, 2007), which is available on the Law Commission's website www.lawcom.govt.nz. That paper contains a detailed analysis and set of references to the literature, which are not repeated here in order to render the arguments more accessible.

3.4 The law of assault and battery, defamation, the tort of passing off, copyright law, protections offered by the law to confidentiality, and the vast amount of law protecting property rights, all protect privacy values to some extent. Thus, one issue is whether laws expressly based on privacy and associated legal remedies are needed, or whether other areas of law are sufficient and contain all that needs to be protected.

TWO MAIN OPTIONS

3.5 In this chapter we discuss two main options for developing a conceptual approach to privacy, each of which is valid for considering the possibilities of law reform. The first option is to see privacy as a subset of certain values. It can then be said that privacy comes from those core values. It is possible to represent the situation by a diagram.

FIGURE 1 – A "CORE VALUES" FRAMEWORK

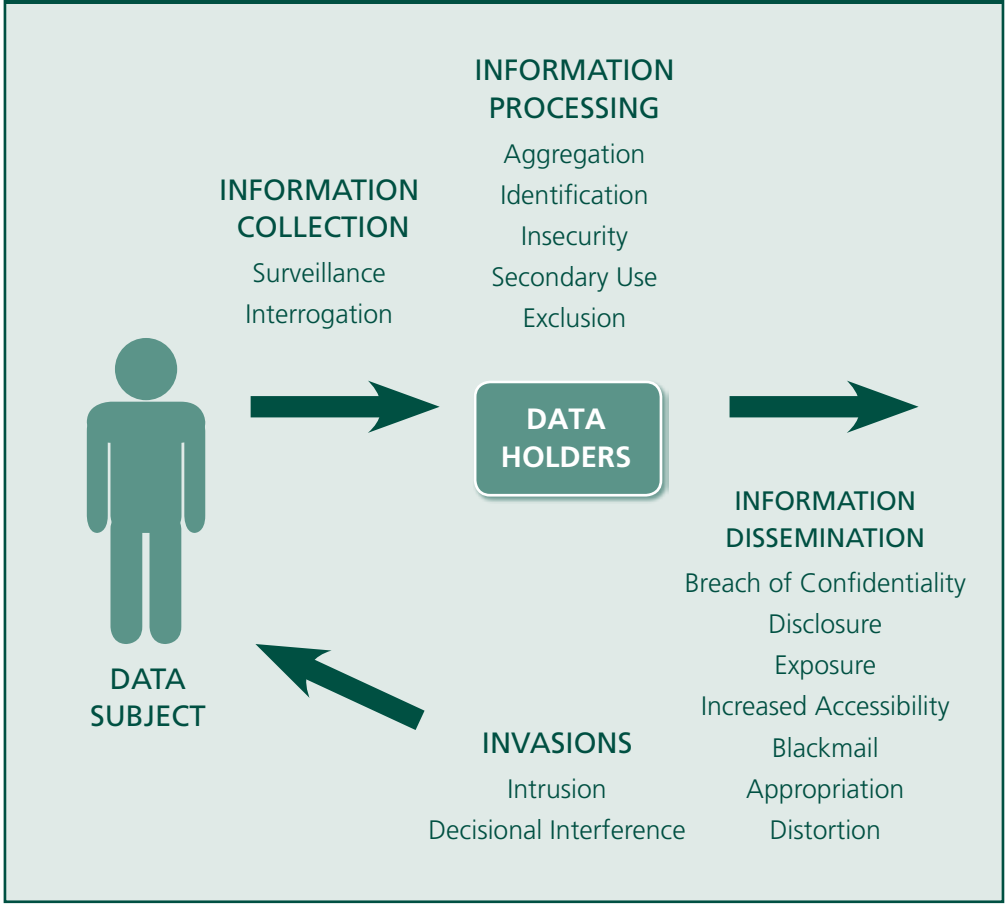


3.6 This figure is intended to show that a moral (or normative) right to privacy is a sub-category of the core values of autonomy and the entitlement of humans to equality of respect. It is a sub-category that overlaps with freedom of expression in the sense that a right to privacy may be supportive of freedom of expression (for instance, allowing solitude for reflection before the freedom of expression is engaged). At other times, the two sub-categories are in tension and may require reconciliation. Because privacy can be supportive of freedom of expression in some circumstances, or in tension with that freedom in others, it is important that the overlap is displayed on the face of the figure. Interests or dimensions of privacy – those in respect of which one ought to have a reasonable expectation of privacy – comprise a further particularised level of

detail falling out of the broad sub-category of a moral right to privacy. The two key dimensions are "local" or "spatial privacy" and "informational privacy". Interests complementary to privacy include questions such as confidentiality, which may collaterally support one's privacy but not necessarily so, and are seldom primarily about privacy explicitly. The figure also shows that, while there is a core of interests or dimensions that will generally fall within the moral right to privacy, there will also be "hard cases" around the edges. Hard cases are those in which it will be difficult to decide whether or not there is a reasonable expectation of privacy in relation to particular matters.

3.7 The second means of developing an analytical framework is to focus on harms to privacy. This model also can be represented diagrammatically.

FIGURE 2 – "TAXONOMY OF PRIVACY"
(from Daniel J Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477, 490)



3.8 In approaching the question of a conceptual approach to privacy through these two options, we have drawn on aspects of those theories discussed in the preceding chapter that we consider to be relatively persuasive. For the first option, we have drawn on those approaches that we categorised in chapter 2 as "personhood" theories. These theories attempt to uncover general values or principles that underlie the concept of privacy – principally values related to humans as beings each of whom requires respect "as a person, as a chooser, … as one engaged on a kind of self-creative enterprise, which could be disrupted, distorted or frustrated even by so limited an intrusion as watching."[6] This sort of observation entwines the value

6 Stanley I Benn "Privacy, Freedom, and Respect for Persons" (1971) 13 Nomos 1, 26.

of equal respect for persons and that of humans as having autonomy, in the sense that each person is able to live and order a life of his or her own choosing. We are of the view that respect for a person's privacy can assist in achieving elements of personhood, such as intimacy and the ability to choose a certain life-path.[7]

3.9 We have adapted the second main option from the approach associated with Daniel Solove: the so-called "pragmatic" approach, which, as discussed in the previous chapter, focuses on identifying privacy harms as disruptions of particular practices, as opposed to exploring underlying values. These disruptions could include, for instance, interference with one's peace of mind, intrusion upon an individual's solitude, or loss of control over facts about oneself.[8] We suggest a way of combining these two options so that they might be seen as working together.

THE CORE VALUES APPROACH

3.10 What we have called the "core values" approach can be organised around the idea of privacy as a sub-category of two interconnected core values:

- the autonomy of humans to live a life of their choosing, and
- the equal entitlement of humans to respect.

3.11 Privacy is seen as a sub-category of these core values because respect for privacy and its value to human beings is conducive to autonomy and equality of respect. For example, privacy assists autonomy by providing a measure of individual solitude and reflection, allowing people to make life choices free from disturbance or scrutiny. By creating a socially-sanctioned space in which people can live free from observation and judgement by others, privacy also ensures equality of respect for the life choices of individuals, even where others might disagree with the content of those choices. To quote David Gauthier in another context, equal respect simply requires that "each respect the identity and aims [as well as preferences or choices] of her fellows, willingly according them equal place in their common affairs with her own".[9]

3.12 A right to privacy can be summed up as protection against unwanted access by other people, where a person has a reasonable expectation of being able to control such access. By "control" we simply mean the power of saying "yes" or "no", although, as with any choice, people do not always get their own way. This approach is not dissimilar to Nicole Moreham's idea that:[10]

> privacy is best defined as the state of "desired 'inaccess'" or as "freedom from unwanted access". In other words, a person will be in a state of privacy if he or she is only seen, heard, touched or found out about if, and to the extent that, he or she wants to be seen, heard, touched or found out about.

7 The value of privacy, including the fashion in which it might assist the development of trust, is considered briefly in Hickford, above n 5, 24-26.

8 Daniel Solove "Conceptualizing Privacy" (2002) 90 Cal L Rev 1087, 1129.

9 David Gauthier "Constituting Democracy" in David Copp, John E Roemer and Jean Hampton (eds) *The Idea of Democracy* (Cambridge University Press, Cambridge, 1995) 318. We recognise that the concept of "equality of respect" is complicated and poses a number of important issues for debate amongst scholars. Readers might wish to refer to the discussion in Kwame Anthony Appiah *The Ethics of Identity* (Princeton University Press, Princeton, 2005) 91-100 and ch 6; and in Charles Taylor "The Politics of Recognition" in Amy Gutman (ed) *Multiculturalism: Examining the Politics of Recognition* (Princeton University Press, Princeton, 1994) 32.

10 N A Moreham "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 LQR 628, 636.

3.13 Thus, the use of the term "control" is intended to signify the desire or intention to exercise such control, as well as the actual exercise of such control. This is different from the factual capability or actuality of control in all cases. Rather, the sense in which it is used here focuses upon whether one *ought* to have the power to determine access to something about oneself, including information. Just because one loses the ability to control access to oneself, this should not mean that one has lost the right to privacy; this point is particularly important given that the technological capability exists to access people without their awareness or consent (see chapter 6). Whether one ought to have privacy, as opposed to whether one actually has it, should be ascertained in terms of how one would wish to exercise a power of control over relative inaccessibility with reference to others if one had full information.[11]

3.14 Nevertheless, as will be discussed below, recognition that privacy is an important human rights value, based upon values of autonomy and equality of respect, does not automatically translate into its recognition as an enforceable legal right in every circumstance. Key issues for consideration in a law reform project are whether there are gaps in the systems of legal protection that now exist, whether those gaps should be filled and, if so, what remedies should be available.

3.15 First, however, we will consider the two main dimensions constituting our understanding of the concept of privacy: the first might be termed "informational privacy"; the second might be characterised as "local" or "spatial privacy".

Informational privacy

3.16 At its core, informational privacy is concerned with control over access to private information or facts about ourselves. John Burrows has observed that "the expression 'private facts' suggests *intimately* private personal facts about me: things such as the state of my health, physical and mental, my intimate bodily appearance, my sexual activity, my family, my domestic relations, and so on".[12] There would probably be general agreement that such facts as these are *usually* private, and that one would have a reasonable expectation to privacy in respect of such things, if that is one's desire. Opinions are likely to differ reasonably on:

- whether certain information may be characterised as "intimately private personal facts" in all factual circumstances or contexts; and
- whether such "intimately private personal facts" or other types of personal information (that would not necessarily be characterised as "intimately private personal facts") should be regarded as worthy of moral or legal protection by way of a right to privacy.

3.17 As certain scholars have observed, the idea of there being certain "intimate" or "private personal" information about oneself in respect of which one would have a reasonable expectation of privacy has intuitive appeal.[13] Advocates of this perspective acknowledge that it is vulnerable to criticism. For instance, Inness notes that her argument in favour of truly private or intimate

11 This discussion is developed in much more detail in Hickford, above n 5, paras 121-126, 133-160.

12 John Burrows "Invasion of Privacy – *Hosking* and Beyond" [2006] NZ L Rev 389, 392 (emphasis added).

13 See chapter 2 above and Julie C Inness *Privacy, Intimacy, and Isolation* (Oxford University Press, New York, 1992) 56-60, for instance, and the discussion on the limitations of using a divide between "intimate" and "non-intimate" information.

information as forming a critical part of the content of privacy is "open to the criticism that I have drawn privacy's content closer to our linguistic intuitions only to abandon our moral intuitions: defining privacy in terms of intimate information, *rather than information as a whole*, fails to account for certain of our moral intuitions".[14]

3.18 It is accepted, then, that it is "generally difficult to define a priori those data that are inherently worthy of greater protection ('sensitive data')".[15] In this vein, Bennett and Raab have cautioned that:[16]

> It is often the shift in context – detaching personal data, through processing, from the circumstances of their original collection – rather than the properties of the data that lead to privacy risks when false conclusions are drawn about persons. In addition, the same information can take on very different sensitivity levels in different contexts. Our names in the telephone directory may be insensitive for most people, but may be very sensitive for vulnerable persons who do not want to be monitored or tracked down.

3.19 We are not claiming that only "intimately personal information" merits moral and perhaps legal protection under the heading of informational privacy, or that such information necessarily deserves greater protection than other classes of information. What we are suggesting is that the inquiry ought to focus upon whether the information is of such a character as to merit consideration as "private" and, if not, whether it is, nevertheless, information regarding which one would have a "reasonable expectation" of privacy in the particular circumstances if that were one's desire. There are dangers in drawing the net of what privacy might relate to either too narrowly or too broadly, so that too many situations are excluded from or included in the class of cases potentially subject to legal action and protection. Burrows notes that the formula of "facts in respect of which I have an expectation of privacy", favoured in the New Zealand case law on the tort of privacy, embraces a more extensive class of information than the "private facts" category referred to above.[17] Certainly, a majority of the Court of Appeal has expressly said so in *Television New Zealand Ltd v Rogers*:[18]

> [W]e are clear the tort is not confined to facts about private life; that is, inherently private matters. Obviously inherently private facts will ordinarily attract a reasonable expectation of privacy. But so may facts which do not have an inherent quality of privacy. We think that is implicit in the observation of Gleeson CJ in

14 Ibid, 58 (emphasis added).

15 Colin J Bennett and Charles Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge (Mass), 2006) 9.

16 Ibid.

17 Burrows, above n 12, 392-393.

18 *Television New Zealand Ltd v Rogers* [2007] 1 NZLR 156 (CA), para 59. See also the decision of the Supreme Court of New Zealand in *Rogers v Television New Zealand Ltd* [2007] NZSC 91 and particularly the comments of McGrath J at paras 100-102 regarding "private facts".

> *Lenah Game Meats* which is reproduced at para[graph] [49] above.[19] That said, we make the obvious point that the privacy value to be attributed to the facts in issue in this case is at the low end of the scale, and certainly much lower than would be the case for inherently private facts. This has importance for the balancing exercise to which we come later in this judgment.

3.20 In the Commission's view, not all information relating to or about a person (personal information) can necessarily be regarded as falling within one's moral entitlement to privacy, and there are legitimate reasons for making some personal information public where society at large might be interested in the transparent disclosure and sharing of such information. Personal information that might not be construed as "private" (or intimately personal), or is assessed to be of such a character that one would not have a "reasonable expectation" of privacy, may, nevertheless, require legal protection (by way of a statutory regime, for example) in order to ensure, say, fairness in dealing with the information or the relevance and accuracy of information held by others. This point calls to mind the observation that policies concerning "identifiable personal information" ought to be (and are) "based inevitably, therefore, on *procedural*, rather than *substantive*, tenets".[20] Bennett and Raab have commented that such policies:[21]

> can put in place the mechanisms by which individuals can assert their own privacy interests and claims, *if they so wish*, and it can impose obligations on those who use personal data. But for the most part, the content of privacy rights and interests have to be defined by individuals themselves according to context.

Local or spatial privacy

3.21 Local or spatial privacy is concerned with control over access to our persons and to private spaces, typically in the home but in other places as well. As Beate Rössler writes: "private life in private spaces follows different rules from life outside these spaces, and these different rules are what permit and promote a different relationship to oneself and a different relationship – different behaviour – towards others".[22] In other words, in our private space we are able to live differently than we do when we are exposed to the gaze of others. It is in these private spaces that we are able to nurture intimate relationships, including family relationships.

---

19 The passage cited from *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 Gleeson CJ was as follows: "There is no bright line which can be drawn between what is private and what is not. Use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford. 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".

20 Bennett and Raab, above n 15, 9 (emphasis in original).

21 Ibid (emphasis in original).

22 Beate Rössler *The Value of Privacy* (Polity, Cambridge, 2005) 142.

3.22 Local or spatial privacy draws resonance from the public belief, first articulated by Sir Edward Coke, that "a man's house is his castle, *et domus sua cuique est tutissimum refugium* [and each man's home is his safest refuge]".[23] This is a bedrock principle of the common law. As Lord Camden LCJ put it in 1765: "By the laws of England, every invasion of private property, be it ever so minute, is a trespass".[24] Many people still regard that idea intuitively as the heart of privacy.

3.23 The home is the usual focus of this dimension of privacy, but not always. One could be away from home in a family vehicle, or with a bag containing personal objects, and have a reasonable expectation that those spaces and items, and indeed one's own body, would remain inaccessible to others. As Moreham has noted:[25]

> "Physical inaccess" … refers to the absence of access to one's person (or to things closely associated with one's person such as one's house, clothes or wallet) either through the use of the senses or through unwanted physical proximity – Y would therefore interfere with X's physical privacy if she installed a video camera in his house, bugged his conversations, broke into his house while he was not there, or rifled through his rubbish bags.

3.24 The question of the extent to which there may be a reasonable expectation of privacy in a public place is a difficult one, and is likely to depend very much on specific circumstances. We discuss privacy in public places briefly in chapter 8, and will return to it in later stages of this Review.[26]

3.25 Interference with local privacy need not involve the acquisition of information, although it may sometimes do so. Intrusion alone is an interference and may come in the form of illicit interference with the subject's actions, illicit surveillance, or illicit intrusions into property.[27]

A HARM-BASED CLASSIFICATION OF PRIVACY

3.26 In spite of the criticisms that we have discussed in chapter 2, the system developed by Daniel Solove is still a useful way of taking the issues into yet further particularity.[28] Solove's taxonomy (or system of classification) in Figure 2 provides a way of considering how the law might protect against specific harms affecting the core values in Figure 1. This study paper adopts a blend of the core values approach and Solove's harm-based approach.

3.27 As we have discussed in chapter 2, Solove focuses upon what he characterises as "harms" to privacy. He includes some categories that are not necessarily legally actionable at all or that are dealt with under legal headings that are not really concerned with privacy. For example, under the information dissemination category he refers to such things as blackmail and distortion (the dissemination of false or misleading information about someone).

23 Sir Edward Coke *The Third Part of the Institutes of the Laws of England* (1628), ch 73.

24 *Entick v Carrington* (1765) 19 St Tr 1029 (Court of Common Pleas).

25 Moreham, above n 10, 649.

26 In particular, we are likely to examine this question in stage 3 of our Review. For one view, see NA Moreham "Privacy in Public Places" (2006) 65 CLJ 606. See also the discussion in Hickford, above n 5, paras 12-14, 117-120, 182-184, which raises some of the difficulties with a conception of privacy in public places.

27 Rössler, above n 22, 9.

28 Daniel J Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477, 522.

3.28 However, Solove's harm-based analysis contains much that is of value in an analysis of privacy. He identifies four distinct groups of activity that may harm a person's privacy. These groupings constitute his taxonomy of privacy. They are:

- **Information collection** in the form of *surveillance* and *interrogation*.
- **Information processing** by *aggregation*; *identification*; *insecurity*, or the careless protection of stored information from leaks and improper access; *secondary use* of the information for a purpose that differs from that for which it was collected; and *exclusion*, or the failure to allow the data subject to know about the data that others have on her and to participate in its handling and use.
- **Information dissemination**. This category involves a range of matters such as *disclosure* (the revelation of truthful information about a person that impacts on the ways others judge her character) and *exposure* (which involves revealing another's nudity, grief or bodily functions).[29]
- **Invasions** of people's private affairs, comprising *intrusion* and *decisional interferences*. Intrusion concerns invasive acts that disturb one's tranquillity or solitude. Intrusion need not involve an incursion into physical space, but can include such things as spam, junk faxes and telemarketing. Decisional interference involves such things as the government's incursion into a person's decisions regarding her private affairs. (This last point arises in the particular legal context of the United States of America – as with the abortion issue – and might be especially controversial in New Zealand law.)

3.29 We believe Solove's broad groupings of potential privacy harms are useful, although, as we have indicated, we do not necessarily see all of his sub-categories as properly falling within the scope of privacy law. Furthermore, there is an argument that his taxonomy is orientated towards "informational privacy" and does not adequately deal with "local" or "spatial privacy".

3.30 The aspects of a blended "core values" and "harms to privacy" approach that we have outlined above demonstrate the complexity of privacy, and also the different perspectives from which it can be approached. The two approaches – one premised on core values, the other addressing harms to privacy – can, we believe, be linked: the first deals with two main dimensions of our expectation that there are areas of our lives that we are entitled to exert control over; the second demonstrates the types of harm against which we should be protected in those areas. There is, however, a considerable philosophical literature on the concept of "harm"[30] and it is not evident whether the concept of "harm" to privacy is engaged at the point of interference itself or whether proof of further tangible damage is required before any legal remedy is required. If the "harm" is indeed the interference (as opposed to any proof of ensuing damage), then there is an issue of whether the interference must be intentional or not. The utility of Solove's perspective for our purposes is that it focuses the attention on the variety of "harms" that might conceivably occur and, as a result, suggests the possible range of activities and consequences that any legal right to privacy would engage with.

29 Other matters included by Solove under information dissemination are breach of confidentiality, increased accessibility, blackmail, appropriation and distortion.

30 For an indication of some of the debates, refer to Joel Feinberg *Social Philosophy* (Prentice-Hall, Englewood Cliffs (NJ), 1973) 25-35.

3.31 In terms of its particular application in given circumstances, privacy is not an absolute. In policy analysis, it is best thought of as a value that will vary substantially depending on what kind of problem or harm is being guarded against, a matter that will require addressing in subsequent stages of the Law Commission's Review. As Solove has put it:[31]

> [T]o understand privacy, we must conceptualize it and its value more pluralistically. Privacy is a set of protections against a related set of problems. These problems are not all related in the same way, but they resemble each other. There is a social value in protecting against each problem, and that value differs depending upon the nature of each problem.

3.32 At this level of particularity – the exposition of harms to privacy – we find this a helpful approach. It prevents the subject of the analysis being "exasperatingly vague and evanescent",[32] while still preserving its connection to the broader core values previously identified.

A LEGAL RIGHT TO PRIVACY

3.33 One question that arises in relation to privacy's legal status is whether there is a right to privacy, or at least a right to aspects of privacy. Further questions then arise. If there is a right, how strong is it? Does that right to privacy or aspects of privacy carry all before it regardless of other considerations? Or is it a weaker form of right that must be balanced against other considerations? Are there other values present in a particular set of circumstances, and what is the relationship of those other values to the privacy values? In other words, does assessing the privacy value involve a weighing against competing considerations? We do not intend to provide definitive answers to all of these questions in this study paper, but we will consider briefly the place that a legal right to privacy might occupy in the law.[33] We also discuss the question of balancing privacy against other values and interests later in this chapter, and in chapter 8.

3.34 The concepts of local privacy and informational privacy already dealt with bear some resemblance to the concerns contained in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms:

> *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 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.

31 Daniel J Solove *"I've Got Nothing to Hide" and other Misunderstandings of Privacy* (George Washington University Law School Public Law Research Paper no 289, 2007) 16.

32 Arthur R Miller *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press, Ann Arbor, 1971) 25.

33 See Hickford, above n 5, ch 6.

3.35 Article 17 of the International Covenant on Civil and Political Rights, a convention that is binding on New Zealand as a matter of international law, has a similar guarantee:[34]

> 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.

3.36 In principle, a legal right to privacy should operate where there are gaps in the protection of the existing law. But there is an issue as to whether it should be allowed to operate where other sources of legal protection might be available and a right to privacy overlaps with those other legal protections. As we have already said, there are a number of existing legal causes of action that protect privacy values without this being their explicit purpose.

3.37 Further legal reform needs to consider whether an actionable legal right to privacy would arise where there has been an infringement or interference with either local or informational privacy resulting in harm or damage, and no other legal remedy is available under statute or common law. For example, the legal protection of the family dwelling house against third parties, through remedies that are available in the legal system now, provides protection for individual and family decisions within that space. The family is allowed to operate within its own realm, leaving what the philosopher John Rawls calls "room for a free and flourishing internal life appropriate to the association in question".[35] This is not to say, however, that the zone of privacy within a private dwelling should protect such things as abuse or neglect of children.

3.38 With any legally actionable right to privacy, there is a live question as to whether the "harm" should be the interference itself or the consequential loss to the aggrieved person, or both. Some torts, such as trespass to land, for example, do not require proof of damage. There is also the question of whether feelings of embarrassment or humiliation should be legally actionable, something the law has been rather reserved about historically. Thus, the question of what amounts to harm for which there should be a legal remedy remains a live issue. But, notwithstanding these difficulties, local or spatial privacy and informational privacy regarding private facts do potentially provide one basis for identifying when a legal right to privacy might be engaged.

3.39 Within any framework there will be peripheral areas, spaces on the margin that are blurred and smudged. The "reasonable expectations" formula (that is, did the person have a reasonable expectation of privacy in the particular circumstances?) is probably helpful as a way of considering these peripheral cases. Such cases could consider what ought to be within one's control, provided one starts with the understanding that the core of privacy in a social world consists of informational privacy over private facts (at least in the first instance)[36] and local or spatial privacy, including control over access to oneself.

---

34 See further discussion in chapter 7 below.

35 John Rawls *The Law of Peoples with "The Idea of Public Reason Revisited"* (Harvard University Press, Cambridge (Mass), 1999) 159.

36 As discussed above.

RISK ANALYSIS AS A POLICY TOOL

3.40 "Risk" is an undeniably complicated concept. It has spawned an extensive literature of its own across a range of subject matter such as insurance, fraudulent activities, health and safety, aviation and environmental degradation.[37] In spite of this literature, however, "risk" remains both problematic conceptually and not necessarily (or readily) quantifiable. The assessment of risks to privacy is not assisted by an absence of agreement as to what "privacy" might mean in given circumstances. Perceptions of risk, even if speculative or misplaced from an objectively measurable point of view, pose problems for those seeking to build trust and confidence in technologies, processes and systems.[38] In certain situations people's fears and impressions can be more potent in governing their behaviour than any objective discernment of risk. For example, people may not want to use their credit cards for transactions over the internet because of their fear that the information may be misused, even though the risk of such misuse may be very low.[39] Public perceptions on these issues matter, and public policy frameworks have to take those perceptions into account.[40]

3.41 Thus, for all systems of data collection and use, the element of trust is very important. In policy terms, then, there is an issue as to whether systems are presumed to be "relatively dangerous" until they can be proved "safe", or whether it is better to wait until harm occurs and then provide a legal remedy.[41] One solution might lie in greater transparency about what technologies and systems can and cannot do, and what protective devices are built into them. Methods, such as "privacy impact assessments",[42] have been developed to assist designers and clients of information-management systems in assessing risk.[43] Such methods cannot escape the profound question of what "risk" is in the context of privacy or personal information, but they might, as Bennett and Raab observe, represent an "improvement upon the one-dimensional notion that there are, a priori, qualitatively and quantitatively undifferentiated 'risks' involving certain types of data, certain types of people, or certain types of practices".[44] Bennett and Raab suggest that further research into privacy risks is needed, and that one obstacle to developing a policy framework is that "mapping the distribution of social attitudes towards these matters as well as patterns of protection in relation to population characteristics is not highly developed".[45] Thus:[46]

37 See for example Ulrich Beck *Risk Society: Towards a New Modernity* (Sage, London, 1992); Ulrich Beck *World Risk Society* (Polity Press, Cambridge, 1999); Ortwin Renn "Three Decades of Risk Research: Accomplishments and New Challenges" (1998) 1 Journal of Risk Research 49; Robert Baldwin and Martin Cave *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press, Oxford, 1999); Malcolm Sparrow *The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance* (The Brookings Institution, Washington DC, 2000).

38 See C Hine and J Eve "Privacy in the Marketplace" (1998) 14 Information Society 253; Bennett and Raab, above n 15, 61.

39 Bennett and Raab, above n 15, 75.

40 We discuss public attitudes to privacy in New Zealand further in chapter 5.

41 Refer to the subtle discussion of this question in Bennett and Raab, above n 15, 61-62.

42 Office of the Privacy Commissioner *Privacy Impact Assessment Handbook* (Wellington, 2007); Information Commissioner's Office (United Kingdom) *PIA Handbook* (2007) available at www.ico.gov.uk (accessed 18 December 2007); Linden Consulting *Privacy Impact Assessments: International Study of their Application and Effects* (report prepared for the Information Commissioner's Office, United Kingdom, October 2007).

43 Bennett and Raab, above n 15, 61.

44 Ibid, 61.

45 Ibid, 76.

46 Ibid, 78-79.

a better understanding of exposures to privacy dangers, the distribution of risks, and the patterning of trusting may be worth seeking. This may be only because discourse based on possible evidence might more clearly delineate the areas of agreement and disagreement between protagonists whose outlooks differ, and what could be accepted as facts upon which a consensus for action could rest. Such discourse might also show the likely range of probabilities and magnitudes of risk, and might establish the plausibility or absurdity of claims in regard to who enjoys, and who does not enjoy, what privacy.

3.42 It has been noted that a "*pre-emptive* as opposed to a *preventative* approach to risk has emerged" in certain areas of policy concern.[47] It is partly this context that leads some commentators to recommend an approach based on dealing fairly with personal information in general, rather than one focused on narrower concepts of privacy.[48] Rather than prescribing in advance the substantive content of privacy in any given situation, various processes or procedures could be established setting out the preferred ways of collecting, holding and dealing with personal information. This approach assumes not only that it is inextricably difficult to ascertain in advance what types of personal information are inherently worthy of legal protection, but also that a procedural approach to regulating handling of such information is preferable in securing desired outcomes.[49]

3.43 The assumption underlying this view may be that "public policy cannot draw a definite line between those types of information that should remain private, and those that may be in the public domain".[50] We have indicated above that the core of informational privacy concerns "intimately private personal facts", although there can be a "reasonable expectation" of privacy regarding other sorts of information in particular contexts.[51] In certain legal instruments, such as the Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981), some types of data have been regarded as more sensitive than others, and special procedures may be laid down for such information.[52] Bennett and Raab have noted, however, that such distinctions remain controversial.[53]

47 Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006) 11 (emphasis in original), referring to F Ewald, "The Return of Descartes' Malicious Demon: An Outline of the Philosophy of Precaution" in T Baker and J Simon (eds) *Embracing Risk: The Changing Culture of Insurance and Responsibility* (Chicago University Press, Chicago, 2002).

48 See, for instance, the discussion in S Simitis "Reviewing Privacy in an Information Society" (1987) 135 U Pa L Rev 707, and Bennett and Raab, above n 15, 8-9.

49 The secondary literature focuses mainly on "informational privacy" rather than "local" or "spatial privacy" (although the processes by which information is gathered may also intrude on local privacy).

50 Bennett and Raab, above n 15, 9. See also discussion in paras 3.16-3.20 above.

51 Burrows, above n 12, 392.

52 Article 6 of the Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data states: "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions".

53 Bennett and Raab, above n 15, 9.

3.44 Clear boundaries can seldom be drawn on normative or legal issues, and context-specific judgements are often required. Rigid definitions prescribed in advance do not assist. We have indicated above that the "core values" approach to the substantive conceptualisation of "privacy" and a process-orientated stance on "fair information" principles can operate simultaneously and focus upon matters that might overlap in practice. That is, adopting one perspective does not necessarily preclude the other.

3.45 Various approaches to assessing the risk of injury or harm have been put forward. In one attempt to distil a theory of negligence applied in United States' appellate court decisions, for instance, reference was made to a three-stage inquiry which a court should try to answer.[54] The first question is, what is the probability of the harm occurring? If it is remote, it may not be thought necessary to guard against it, unless the likely consequences of it occurring would be very serious. The second question is, what is the magnitude of the harm should it occur? How grave or serious will be the resulting injury? The third leg of the inquiry is to discover how to avoid the risk, and what the costs may be of taking steps to neutralise or minimise it. On this sort of analysis, if the answer or product of the first two questions "exceeds the burden of precautions, the failure to take those precautions is negligence".[55]

3.46 The retrospective analysis of "risk" can be useful for assessing liability in litigation concerning personal injury or alleged invasions of interest, and for deciding on *remedial* legal and policy actions.[56] Identifying harm that may occur in the future requires something different, however – a preventative approach (or perhaps a "pre-emptive" one). Context is important when assessing the risk of future harm, especially in circumstances where there might not be agreement on how to quantify the "risk" or on what the "harm" might be. In relation to risks to privacy, different people weigh the values at stake in these issues differently. Survey research reveals that in the United Kingdom there are three broad groups of people:[57]

- those who are unconcerned about privacy and are willing to provide or allow collection of personal information by organisations;
- privacy pragmatists, who are prepared to make explicit trade-offs by providing personal information in return for specific benefits such as better service or discounts; and
- privacy fundamentalists, who are unwilling to provide personal information except in situations in which they can exercise a high degree of control over who uses their information and for what purposes it is used.

54 Richard Posner "A Theory of Negligence" (1972) 29 Journal of Legal Studies 32, 33, referring to the approach of Justice Learned Hand in *United States v Carroll Towing Co* 159 F 2d 169 (2nd Cir 1947).

55 Ibid.

56 Relying upon approaches formulated in common law merits some caution, as litigation develops in an episodic manner and may be somewhat inadequate on its own for assisting a relatively systemic preventative or precautionary approach to "risk". On the infirmities of case law in this context see Hon Leslie Scarman "Codification and Judge Made Law: A Problem of Coexistence" (1966) 42 Indiana LJ 355, 366; Mary Arden "Time for an English Commercial Code" [1997] CLJ 516, 534; Lord Cooke "Party Autonomy" (1999) 30 VUWLR 257, 264.

57 Perri 6 *The Future of Privacy* (vol 1, Demos, London, 1998) 44.

3.47 Solove, following Lawrence Lessig, introduces the concept of "architecture" as a means of throwing light on how some privacy problems should be dealt with.[58] Lessig has observed that:[59]

> [T]he nature of the Net is set in part by its architectures, and … the possible architectures of cyberspace are many. The values that these architectures embed are different, and one type of difference is regulability – a difference in the ability to control behavior within a particular cyberspace. Some architectures make behavior more regulable; other architectures make behavior less regulable.

3.48 Computer architecture for the collection, storage and retrieval of data has a profound effect on how the systems perform. Such architecture can create a feeling of vulnerability in individuals, expose them to dangers such as identity theft, and disempower them. An architectural approach to privacy does not concentrate on individual remedies for invasions. The purpose is to produce systems that are more secure, safe and trustworthy so that the downsides of the new technology are minimised. Solove suggests that such an approach would establish controls over data networking practices in institutions and would afford people greater participation in the uses of their information.[60] This may involve a redefinition of the relationships between business and government entities that maintain and use the information of individuals. The aim of a new architecture built around participation and responsibility is to prevent abuses occurring in the first place.[61] These insights appear to us to be the basis for a fruitful policy approach.

3.49 Other analysts have also dealt with the question of how risk can illuminate the problems of privacy. The study into *The Future of Privacy* published by Demos in the United Kingdom looks at informational privacy through the lens of risk, and categorises risks to privacy under three headings:[62]

- **Risks of injustice:** Organisations may wish to use personal information for purposes other than those for which it was collected and to disclose it to others without consent. There could be a risk of injustice from this if there is significant inaccuracy in the information that may led to unjust treatment for the individuals to whom the information relates. If data gathered for one purpose is used for other purposes, incorrect inferences may be drawn. People may fall under unjustified suspicion and be regarded as guilty of conduct in which they have not engaged.
- **Risks to personal control over collection of personal information:** For example, as we discuss in chapter 6, data is captured from people who visit websites, without their knowledge or consent. This can lead to excessive or unjustified surveillance, which traces and profiles people, their attitudes and contacts. People may be left without any means of controlling the collection of their personal information, or of protecting themselves against risk.

---

58 Daniel J Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2004) 97. Lawrence Lessig was a major source for the use of the concept of "architecture": see *Code and Other Laws of Cyberspace* (Basic Books, New York, 1999) 26-27 and ch 4. See also Bennett and Raab, above n 15, 181-182, 183-184, 287-288.

59 Lessig, above n 58, 30.

60 Solove *Digital Person*, above n 58, 102.

61 Ibid, 123

62 6, above n 57, 40-42.

- **Risks to dignity by exposure and embarrassment:** Exposure and disclosure of some information can lead to a loss of dignity and reputation for the person concerned. There may be no reason to make the information available for any public purpose. There may be no transparency in the disclosure: the subject may not know it is going to happen and may not be told that it has happened. There may be collection of information that is essentially private, and exposure of a person's identity in connection with the information for no valid reason.

THE LAW COMMISSION'S VIEW

3.50 In our view, privacy is an important and indispensable value in modern society,[63] but it is not an absolute right. It has to be weighed and reconciled with other values, including values that have to do with the public interest. Freedom of expression is one of the most prominent of those other values. There are points of tension between privacy and other values, and this needs to be recognised, as we explore further in chapter 8.

3.51 What is called for is a proper weighting of the relevant values in the particular circumstances in which they arise. This means that in different areas of human activity, different weighting may be appropriate. For example, it may be necessary for the proper conduct of the land transfer system that there be a public register identifying the registered proprietors of all land in New Zealand. On the other hand, it may not be appropriate for a person's medical record to be posted as public information on the internet. Health information may be in a quite different category from land information. The public interests in the two situations are different, the analysis is different, and the outcome will be different. In many ways, therefore, the task in front of the Law Commission is to consider how privacy and other values should be weighed in different contexts.

3.52 In some areas the privacy value and the need for it are clear, and the policy argument is about how to intervene to achieve the necessary protection in an effective manner. In this area, the instrument choice questions are difficult.

3.53 It is widely recognised that there is a need for some regulation of data collected and held by government and the private sector in order to protect information relating to individuals. This seems to us to be a core area of public and policy concern. It is addressed in the Privacy Act 1993 in New Zealand, and a framework of policy is developed in that Act for dealing with that problem. Thus, the issue in the area of data protection is not whether it is necessary but rather how it should be carried out as efficiently and effectively as possible. The Law Commission will review that framework when it gets to stage 4 of its Review of Privacy, but the need for a framework can hardly be doubted.

3.54 When it comes to the emerging tort of invasion of privacy in New Zealand a different set of values fall to be weighed than those that are weighed in the data protection area. The privacy tort is a relatively open-ended and undefined framework as matters stand. Yet, it is clear that there are values such as freedom of expression that need to be weighed in any framework that is developed for dealing with the possibility of a civil action in tort based on breaches of privacy. Thus, the tests for developing policy settings for a broad tort remedy are rather different from those relating to the regulation of stored data.

63 See Hickford, above n 5, 24-26.

3.55 It is the Law Commission's view that a broad, comprehensive and all-embracing approach to privacy is a mistake. What is required is a careful analysis of each topic where the issue arises. This involves weighing the competing factors and deciding whether legislation or some other regulatory response is required.[64] If it is, it then becomes a question of deciding what sorts of features the preferred regulatory regime should have, bearing in mind that a blend of legislative and non-legislative options might be appropriate. In our view this sort of analysis needs to be conducted in each policy area. Otherwise we will end up with an unpredictable general privacy law of little utility and dangerously uncertain breadth of application.

3.56 The Commission is attracted to the view advanced by its President as long ago as 1975:[65]

> All legislative and judicial decisions represent a balance between competing values and objectives. On some occasions privacy should weigh heavily in the balance, on other occasions there will be more important countervailing values. I am saying nothing more profound than that our approach to privacy should be piecemeal.

3.57 In view of the foregoing, the Law Commission believes that it is not likely to be productive to search for a generalised privacy law lacking specificity. Where a need for legislative intervention has been demonstrated, it should proceed with a specifically-targeted law. The approach to privacy protection needs to be particularised, not generalised. Where there are demonstrated problems and abuses, interventions should be made, but not otherwise.

64 For a discussion regarding the difficult analytical and policy issues underlying the assumptions of "weighing", "reconciling" or "balancing" different dimensions of value, see for example Charles Raab "From Balancing to Steering: New Directions for Data Protection" in Colin J Bennett and Rebecca Grant (eds) *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, Toronto, 1999) 68; and Bennett and Raab, above n 15, 5-6, 13, 243-244, 295. Bennett and Raab (ibid, 13) state that: "Although the concept [of balance] is related to the terminology of judicial decision, the achievement of a balance may ultimately be a matter of political negotiation, perhaps arriving at a consensus; or, alternatively, of authoritative assertion."

65 Geoffrey Palmer "Privacy and the Law" [1975] NZLJ 747, 748.

Chapter 4:
Privacy in Law

4.1 In this chapter we trace the development of privacy in New Zealand statute and common law.[1] Up until the last quarter of the 20th century, privacy was largely a "silent" value in the law, present in certain situations but unexpressed. The common law traditionally eschewed a freestanding privacy right unconnected with direct interference with property rights, liberty and bodily integrity.[2] Aspects of privacy protection, both local and informational privacy, can nevertheless be discerned in legal actions such as the common law torts of trespass, assault and nuisance, and in various discrete statutory provisions protecting property and prohibiting certain disclosures of information.[3] Although patchy and erratic in the protection of privacy, these measures suggest that "privacy has been recognised for a long time as an underlying value worth protecting, even if that protection has been partial and very poorly articulated."[4]

4.2 Privacy as a legal issue "arrived in New Zealand by osmosis" from overseas.[5] Writing in 1975, Geoffrey Palmer noted that the amount of New Zealand legal scholarship in the field was very slender.[6] Around that time, however, a trend towards expressly acknowledging aspects of privacy in both statute and case law was established, with privacy becoming a legally enforceable value in its own right. Examples include the Human Rights Commission Act 1977, the Broadcasting Acts 1976 and 1989, the Official Information Act 1982 and the Privacy Act 1993. Judicial decisions started to mention privacy expressly. The developing emphasis on privacy responded largely to social concerns about the growth of government, the growth of the mass media and technological changes.[7]

1 Mention is also made of English and Australian cases and relevant law from other jurisdictions for illustrative purposes.

2 A Butler & P Butler *The New Zealand Bill of Rights Act* (LexisNexis, Wellington, 2005) ch 3, fn 41; P Rishworth, G Huscroft, S Optican and R Mahoney *The New Zealand Bill of Rights* (Oxford University Press, Oxford, 2003) 309.

3 See *Halsbury's Laws of England* (4 ed reissue) vol 8(2) Consitutional Law and Human Rights, para 110.

4 John Burrows "Invasion of Privacy" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 745.

5 Geoffrey Palmer "Privacy and the Law" [1975] NZLJ 747.

6 Ibid.

7 EH Flitton and G Palmer "The Right to Privacy: a Comparison of New Zealand and American Law: Part II" (1968) 3 Recent Law 149, 159.

4.3 This chapter is concerned with the development of privacy in the law. We have not examined ways in which the law interferes with or fails to adequately protect privacy. Neither do we identify gaps that may exist in privacy protection; we will come to those at a later stage in the Commission's Review of Privacy.

PRIVACY: A SILENT VALUE IN THE LAW

4.4 A range of legal provisions have had the ancillary consequence of protecting aspects of privacy, although privacy itself is an unnamed rationale in the period up until the mid-1970s. These provisions include statutes creating offences to protect the possession of land and prohibit the disclosure of certain information, as well as various torts recognised by the common law.

Statute law

Local privacy

4.5 For many years, the criminal law has regulated certain types of privacy invasions by creating criminal offences for particular actions or behaviours that impact on individual privacy to an unacceptable degree. In 1927 it was for the first time made an offence to be found on property without lawful excuse.[8] This was probably less about privacy than it was about protecting possession of land, always dearly prized at common law. It was also doubtless aimed at the prevention of other offences such as theft and burglary. It appeared in a part of the Police Offences Act 1927 under the heading "Rogues and Vagabonds". However, it was something akin to personal privacy that in the view of some historians lay behind the protection of possession of land.[9] There is judicial acknowledgment that the section was at least in part meant to protect against invasion of privacy.[10] It was not until 1960 that it was made an offence to "peep or peer" into the window of a dwelling-house, a provision obviously targeted at the so-called peeping tom.[11]

Informational privacy

4.6 There was surprisingly little statute law in the first part of the 20th century that could be said to protect privacy by limiting disclosure, and even then those early statutes may have been grounded primarily in values other than privacy. The first statutory provision indirectly prohibiting the disclosure of personal information appeared in 1884 in an Act regulating the telegraph service. It rendered it an offence to disclose the contents of any telegram or telegraph (which may or may not have included personal information).[12] This was extended to letters in 1919.[13]

8 Police Offences Act 1927, s 54, now Summary Offences Act 1981, s 29.

9 See Frederick Pollock and Frederic William Maitland *The History of English Law* (vol II, 2 ed, Cambridge University Press, Cambridge, 1968) 41-42. Pollock and Maitland said that some believed the disturbance of possession of land was "an invasion of the sphere of peace and quiet which the law should guarantee to every one of its subjects".

10 *Carpenter v Police* [1969] NZLR 1052, 1053 (SC) Wild CJ.

11 Police Offences Act 1927, s 52A, added in 1960; now Summary Offences Act 1981, s 30.

12 Electric Lines Act 1884, s 30.

13 Post and Telegraph Amendment Act 1919, s 13.

Again, it is not clear that privacy was the sole driver; the position of the provisions in the Act suggests they were as much concerned with preventing theft and sabotage. The first statutory provision which clearly protected intimate personal information was a section added in 1944 to the legislation on hospitals which rendered it an offence for health workers to disclose the health details of anyone in hospital.[14]

4.7 There were also a number of Acts dating back to the early 20th century that prohibited persons in certain sorts of employment from disclosing information which came into their possession in the course of their employment. They included officers of the Post Office Savings Bank who were required to maintain secrecy about the state of their clients' accounts,[15] and the staff of the Public Trust Office who were forbidden to disclose anything pertaining to the business of the Trust, in particular the details of any estate under administration in that office.[16] These express statutory provisions criminalised breaches of confidence by people in certain positions, but probably imposed no higher a duty than the common law already imposed on professionals in relation to their clients by way of a duty of confidence.

4.8 The Report of the Danks Committee on Official Information included a list of statutory prohibitions on the disclosure of official information (in many cases to protect individual privacy), enacted in the period from the 1950s through to the 1970s. These prohibitions related to such matters as education information, complaints about safety issues, electoral and polling secrecy, adoption records, prison records, and social welfare information.[17]

4.9 In a number of instances, information disclosed under legal compulsion was protected: the legislation was designed to ensure that someone who was required to divulge personal or financial details could be assured of confidentiality. The Inland Revenue Department[18] and the Department of Statistics[19] were examples. These provisions should also be viewed in the context of the general secrecy of information held by Government under the Official Secrets Act 1951.

4.10 In sharp contra-distinction to this, from an early time a number of government departments and agencies were required by statute to maintain public registers, and as a general rule those registers were public documents which could be searched by anyone. Some of them contained details which some individuals might regard as their own business. From the District Land Register, for example, it was possible for anyone to discover the amount of a mortgage on someone's land, or what the owner had paid for the property. The births, deaths and marriages registers reveal details of a person's date of birth, parents, and date and cause of death.[20]

---

14 Statutes Amendment Act 1944, s 31.

15 Post Office Act 1900, s 72. Compare the banker's common law duty to the client: *Tournier v National Provisional Bank* [1924] 1 KB 461.

16 Public Trust Office Act 1957, s 17.

17 Committee on Official Information *Towards Open Government Supplementary Report* (Wellington, 1981) Appendix 4; noted in *Hosking v Runting* [2005] 1 NZLR 1, para 189 (CA) Keith J.

18 Land and Income Tax Act 1923, s 6, now Tax Administration Act 1994, ss 81-89.

19 Statistics Act 1955, s 18, now Statistics Act 1975, s 21.

20 The public right to search the District Land Register dates back to 1870, and the births deaths and marriages registers to 1847. See New Zealand Law Commission *Public Registers* (NZLC IP3, Wellington, 2007) paras 25, 32.

Common law

4.11 The common law did not recognise a right of privacy per se; however, this has not prevented the courts from acknowledging that privacy values underlie and inform other rules of law.[21] It has been the case for a long time that sometimes what might be classified as an infringement of privacy could be redressed under some other head of the common law. For example, violations of one's bodily integrity have traditionally been protected by specific criminal offences or civil actions such as assault, battery and negligence.[22] In relation to privacy of the home, the torts protecting possession of land (trespass and nuisance), which are of ancient origin, are strict liability torts which evidence the importance that the law has always placed on possession of real property. In relation to disclosure of personal information, possible causes of action, depending on the circumstances, have included breach of confidence,[23] negligence,[24] copyright,[25] defamation,[26] malicious falsehood,[27] and the tort of passing off.[28]

4.12 The action for breach of confidence, which had its origins in equity, most often provided a plaintiff with a remedy for invasion of privacy. It most commonly arose out of a relationship between two persons in which one entrusted information to the other in confidence, in other words, on the understanding that the recipient would not disclose it to others. Thus, the relationship between a banker and a client, and a lawyer and a client, was one of confidence. So too was that of employer and employee in some cases, where in the course of employment the employee was entrusted with the trade secrets of the business. There are also cases establishing that the breach of confidence action will protect domestic confidences, including matrimonial confidences,[29] and details of an employer's home and family life.[30] However, while the great majority of confidence cases involved a relationship of some kind, it was not a necessary requirement. From an early stage, it was recognised that an obligation of confidence might attach because of the circumstances in which the information was acquired; for example, if it had been stolen, or obtained in a surreptitious manner. In such cases equity would impose an obligation on the conscience of the recipient just as if he or she had been entrusted with the information.[31]

---

21 *Wainwright v Home Office* [2004] 2 AC 406, 419 (HL); Brian Neill "Privacy: A Challenge for the Next Century" in Basil S Markesinis (ed) *Protecting Privacy* (Oxford University Press, Oxford, 1999).

22 Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (The Federation Press, Sydney, 2005) 5.

23 For recent discussion of the doctrine, see *Anne Hunt v A* (6 August 2007) CA 114/06.

24 *Furniss v Fitchett* [1958] NZLR 396 (SC).

25 *Williams v Settle* [1960] 1 WLR 1072.

26 *Tolley v Fry* [1931] AC 333 (HL); *Kirk v AH & AW Reed* [1968] NZLR 801 (CA). For a more recent authority, see *Ettinghausen v ACP* (1991) 23 NSWLR 443 (SCNSW).

27 For a modern decision relying on this tort, see *Kaye v Robertson* [1991] FSR 62 (EWCA (Civ)).

28 For discussion of privacy protection by the common law under various heads of liability, see Palmer, above n 5, 749-751; Gerald Dworkin "The Common Law Protection of Privacy" (1967) U Tas LR 418, 422-427; Burrows, above n 4, 745-748; Neill, above n 21, 4-12; R Glanville Glover "The Right to Privacy (1983) Canta LR 51, 54-57. In relation to privacy and copyright, see Susy Frankel "The Copyright and Privacy Nexus" (2005) 36 VUWLR 507.

29 *Argyll v Argyll* [1967] Ch 302.

30 The cases involving the royal family and their domestic staff are good examples; *Prince Albert v Strange* (1849) 1 McN & G 23; 2 DeG & SM 293, 313 Knight Bruce VC: a case of "sordid spying into the privacy of domestic life."

31 *Ashburton v Pape* [1913] 2 Ch 469; *Phillip v Pennell* [1907] 2 Ch 577.

4.13 From an early time, the common law and equity therefore sometimes protected privacy, but were only able to do so in the confines of other established causes of action. There were many situations where those causes of action did not fit, and where the plaintiff was left without a remedy.

Court proceedings

4.14 In earlier times, there seems to have been little concern for the privacy of those engaged in court proceedings, even proceedings involving the disclosure of deeply personal information. For example, in the first half of the 20th century, proceedings for divorce normally took place in open court. Statute conferred power on judges to try cases in chambers, but the only statutory ground for doing so was that hearing the case in open court would not be in the interests of public morals.[32] The sensibilities of the parties played no part in that decision. This was no doubt due in large part to the fact that divorce in those times was fault based. As Edwards J said in 1917:[33]

> At all events it cannot be in the interest of public morals that persons, because they are well known and because their offences are gross, should be assisted by the Court to hush up, so far as possible, the knowledge of their offences.

4.15 Publication of details could also be prohibited by the court in divorce cases, although once again the ground was public morals rather than any distress publication might cause to the parties. However, orders suppressing publication were not so uncommon because, as Edwards J said:[34]

> Rarely, if ever, can it be in the interest of public morals that the details of divorce proceedings shall be published for the delectation of persons who desire to gloat over such unsavoury matter.

4.16 The pattern was much the same in criminal cases. From early times there was power to clear the court and to forbid publication of reports, but the privacy of a participant was not in itself a ground for doing so. In 1908, "public morals" was the only ground. In 1961 the grounds were expanded to:[35]

> the interests of justice or of public morality or of the reputation of any victim of any alleged sexual offence or offence of extortion, or the security or defence of New Zealand.

In other words, even in 1961, the protection of individuals was confined to cases where their *reputation* was at stake.

4.17 It is notable, however, that the interests of children were better protected from an early time. If a judge felt that young children could be prejudiced by their parents' divorce proceedings being heard in open court, he would more readily order a hearing in chambers.[36] Even then it was not until the Guardianship Act 1968 that

32 See the Divorce and Matrimonial Causes Act 1908, s 65.

33 *T v T* [1917] GLR 334 (SC).

34 Ibid.

35 Crimes Act 1908, s 432; Crimes Act 1961, s 375. The latter provisions remain in force: Criminal Justice Act 1985, s 138.

36 *T v T*, above n 33.

there was an unequivocal statutory direction that matters involving the custody of children be heard in private.[37] In 1974, it was made an offence to publish the name of any witness in a criminal case who was under the age of 17 years.[38] As early as 1925, children appearing in the Children's (later the Youth) Court, were also shielded from publicity: there could be no reports of proceedings in that court without the judge's consent, and in no case could the young person be identified.[39]

Attitude of the law to claims for mental distress

4.18 One may ask why in earlier times our legal institutions, in particular the courts, were so unwilling to recognise privacy as a legal right. John Fleming in his famous work on torts said this:[40]

> The violation of privacy has not so far, at least under that name, received explicit recognition as a tort by British courts. For one thing, the traditional approach has been to formulate tort liability in terms of reprehensible conduct rather than of specified interests entitled to protection. For another, our courts have been content to grope forward cautiously along the grooves of established legal concepts, like nuisance and libel, rather than make a bold commitment to an entirely new head of liability. Some of this hesitation is undoubtedly due to the fact that we are here concerned primarily with injury in the shape of mental distress, which has so frequently evoked the fear of opening the door to fanciful claims. Another factor is the difficulty of drawing a clear line between what should and should not be tolerated. The mere fact of living in the crowded society of today exposes everyone to annoying contacts with others, most of which must be borne as the price of social existence. Also, free speech and dissemination of news are important competing values, and it is only when intrusion becomes intolerably offensive by prevailing standards of taste and propriety that legal intervention would become warranted.

4.19 Fleming's difficulty of drawing the line is a reflection of the nebulous and uncertain definition of privacy to which we have referred earlier. But his emphasis on the type of damage which flows from an invasion of privacy is also worthy of note. In many cases it is mental distress in the form of embarrassment and humiliation, and the common law was long unwilling to redress such indeterminate damage as this.[41] In 2005 Todd, writing about the law of negligence, was still able to say that "mere upset, grief or distress do not give rise to any cause of action".[42]

THE PRIVACY ERA: RECOGNITION OF PRIVACY

4.20 Notwithstanding the law's traditional reluctance to expressly recognise privacy, the legislature and the courts of New Zealand have progressively moved to a position where privacy is recognised, not just as an important social value but as one which the law should protect. Several inter-related developments have been instrumental in this movement.

37 Guardianship Act 1968, s 29. Reporting of proceedings in the Family Court is now governed by the Care of Children Act 2004, s 139.

38 Children and Young Persons Act 1974, s 97 (now repealed but replaced under the Criminal Justice Act 1985, s 139A).

39 Child Welfare Act 1925, s 30.

40 JG Fleming *The Law of Torts* (9 ed, Law Book Company, Sydney, 1998) 664-665.

41 See the judgment of Lord Scott in *Wainwright v Home Office*, above n 21, para 62, for a modern reiteration of this view.

42 Stephen Todd "Negligence: The Duty of Care" in Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed, Brookers, Wellington, 2005) 114, 158.

4.21 First, the rapid advance of new technologies has engendered real fears in many people about others gaining access to their private information without their knowledge. The 1970s heralded the growth of the computer industry, and with it came an increasing awareness of the need for a more generalised privacy protection.

4.22 Second, international conventions, in particular the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention on Human Rights have written privacy large among the rights that they protect.

4.23 Third, our human rights legislation, in particular the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993 (the successor to the Human Rights Commission Act 1977) have increased public awareness of the dignity of the individual. If discrimination on grounds of race, religion and gender are matters about which the law should be concerned, why not the distress caused by breach of privacy?

4.24 Finally, in other areas the law has progressively begun to recognise mental distress and injury to feelings as heads of damages. In malicious falsehood,[43] the law of contract[44] and employment law,[45] for example, that has become accepted. The traditional antipathy of the law towards compensating mental distress is therefore lessening, opening the way for the granting of damages for invasions of privacy.[46]

A general statutory right of privacy?

4.25 Towards the end of the 1960s there were a number of attempts in the United Kingdom to pass private members' bills that would have introduced a statutory right of privacy. A Right of Privacy Bill (dealing with intrusions by the media) was introduced in the House of Lords in 1961 by Lord Mancroft. Another Right of Privacy Bill, presented to the House of Commons by Mr Lyon in 1967, proposed a statutory right of action for infringement of privacy. A further Right of Privacy Bill was presented to the same House by Mr Walden in 1969, based on a draft Bill prepared by Justice (the British section of the International Commission of Jurists) as part of a report that had recommended the statutory enactment of a right of action for infringement of privacy.[47] Debate on that Bill led to the Younger Committee report in 1972 that rejected the idea of a statutory general right of privacy, on the basis that the courts may have difficulty balancing privacy with competing interests such as freedom of information.[48] Minority reports, however, were of the view that the courts could resolve the difficult questions of balance of interests posed by general privacy legislation.

---

43 *Khodaparast v Shad* [2000] 1 WLR 618 (EWCA (Civ)).

44 *Snodgrass v Hammington* (1995) 10 PRNZ 672 (CA).

45 Employment Relations Act 2000, s 123(c).

46 See *Hosking v Runting*, above n 17, para 128 Gault P and Blanchard J, discussed more fully at paras 4.74-4.78 below.

47 Justice, British Section of the International Commission of Jurists *Privacy and the Law* (Stevens & Sons Limited, London, 1970).

48 Report of the Committee on Privacy (1972) Cmnd 5012. The Younger Committee was limited by its terms of reference to consideration of privacy issues in the private sector. See Hon H Storey "Infringement of Privacy and its Remedies" (1973) 47 ALJ 498, 507-508.

4.26 In two Canadian provinces, privacy legislation was successfully enacted at this time. British Columbia and Manitoba enacted Privacy Acts (1968 and 1970 respectively) providing a statutory tort for invasion of privacy.[49] In Queensland, the Invasion of Privacy Act 1971 dealt with certain privacy issues involved with the granting of credit, as well as listening devices and private investigators.

4.27 Around this time, there were no such attempts in New Zealand to address privacy in a general way by statute, influenced no doubt by the lack of initial success in introducing any such legislation in the United Kingdom.[50] However, consideration was given to the privacy implications of the growing use of computers in New Zealand society, discussed below in relation to informational privacy. In addition, statute law in New Zealand continued to address specific privacy issues.

Statute law

Local privacy

4.28 From the mid-1970s, specific statutory controls continued and multiplied, although for the most part they have been narrowly targeted. In 1974 it became an offence for a private detective to photograph, film or videotape a person, or record a person's voice, without that person's consent.[51] In 1997, the Harassment Act introduced both civil and criminal penalties for various types of harassment. Among the conduct which can constitute harassment is watching another person's residence; entering a person's property; or making contact with the person by telephone, correspondence, or in any other way.[52] In 2006 it was rendered an offence to covertly make a visual recording of someone while they are in an intimate situation.[53]

4.29 In relation to authorised privacy intrusions by law enforcement or regulatory powers of search and entry, many statutes recognise that the home and the person are particularly sensitive zones of privacy.[54] For example, section 200 of the Fisheries Act 1996 allows the exercise of the power of entry onto a private dwelling or onto a Māori reservation only if the officer is authorised to do so by a District Court Judge.

49 See Storey, above n 48, 506-507. Three further Canadian provinces (Saskatchewan, Newfoundland and Quebec) have subsequently introduced statutory causes of action for invasion of privacy: New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC CP1, Sydney, 2007) 82.

50 A right of privacy was subsequently considered but rejected in relation to the enactment of the New Zealand Bill of Rights Act 1990: see further below. The United Kingdom eventually enacted a right of privacy by adopting Article 8 of the European Convention on Human Rights in the Human Rights Act 1998 (UK); see further chapter 7.

51 Private Investigators and Security Guards Act 1974, s 52. The long title provides that one purpose of the Act is "to provide for the licensing of private investigators as a means of affording greater protection to the individual's right to privacy against possible intrusion by private investigators."

52 Harassment Act 1997, ss 3 and 4. In *Hosking v Runting*, above n 17, para 108 Gault P and Blanchard J noted that this provision clearly recognises the privacy value and entitlement to protection.

53 Crimes Act 1961, ss 216G-216N, inserted by the Crimes (Intimate Covert Filming) Amendment Act 2006.

54 Butler and Butler, above n 2, paras 3.4.29, 18.29.31.

Informational privacy

4.30 In the early 1970s, the growing use of computers created the impetus for a number of attempts to introduce legislation regulating informational privacy, including the Data Surveillance Bill 1969 (UK), the Personal Records (Computer) Bill 1969 (UK), the Control of Personal Information Bill 1971 (UK), the Data Privacy Bill 1972 (Canada), and the Information Storages Bill 1972 (Vic).[55] However, none of these early attempts to introduce such legislation proved to be successful.

4.31 There were also concerns in New Zealand about the privacy implications of the storage of information in computers. In May 1972, the New Zealand Computer Society published a report entitled *Investigation of a Unique Identification System*. Mr Drayton introduced the Preservation of Privacy Bill in 1972 "to preserve individual privacy and to prevent storage and distribution of incorrect personal information in and from computer memory banks." The Bill proposed the establishment of a Privacy Commissioner to register all computer installations in New Zealand, including the nature of the data stored in each installation and the purpose for which it was stored. It was also proposed that everyone about whom information was stored would receive a print-out of all information stored about them. However, the Bill did not proceed pending a report by the Law Revision Commission sub-committee on computer data banks and privacy.[56]

4.32 In the 1970s and 1980s, Parliament moved beyond narrowly-targeted protections for the first time, and signalled that privacy was a value which merited general legal recognition, although generally this was to be achieved through mechanisms other than the courts.[57] The Wanganui Computer Act 1976 prescribed stringent security measures around the Wanganui Computer Centre.[58] This Act established a Policy Committee and empowered it to determine the policy of the Centre relating to the privacy and protection of the rights of individuals.[59] The State Services Commission and the departments concerned had to take all reasonable steps to ensure that unauthorised persons did not have access to the computer, and a Privacy Commissioner was appointed to oversee the operation of the system.

4.33 In the criminal context, in 1979 a new Part 9A was added to the Crimes Act 1961 titled "Crimes against personal privacy".[60] This includes an offence of using a listening device to intercept someone else's private communication,[61] a provision which was much more recently extended to any form of interception

55 See Storey, above n 48, 513; the Law Revision Commission *Report of Sub-Committee on Computer Data Banks and Privacy* (1973) 24.

56 Law Revision Commission, above n 55.

57 For a timeline of information privacy law developments in New Zealand 1974-1994, see Elizabeth Longworth and Tim McBride *The Privacy Act: A Guide* (GP Publishing, Wellington, 1994) 26-29.

58 The Wanganui Computer Act has been repealed and access to information formerly held on the Wanganui Computer (details of criminal convictions, court hearings, fines and orders; details of firearms, deportation orders and overseas convictions; details of traffic offence demerit points, and licensing offences; and the national register of drivers' licences, motor vehicles and transport licences) is now regulated by the Privacy Act 1993 and other statutes.

59 Described in *Hosking v Runting*, above n 17, para 191 Keith J, as a most uncommon statutory reference at that time to "privacy."

60 Part 9A also includes offences involving intimate visual recordings (sections 216G to 216N of the Crimes Act 1961), referred to in relation to local privacy in para 4.28 above.

61 Crimes Act 1961, ss 216A-216F, added in 1979.

device.[62] The definition of "private communication" involves an expectation of privacy so that a communication will be considered private if any one party to it desires it to be confined to the parties,[63] although there is an exception permitting the recording of a private communication by a party to the communication.[64] Offences relating to computer hacking have also been introduced.[65]

4.34 As well as creating offences for actions that impact on personal privacy, the Crimes Act 1961 also allows regulated exceptions to these offences for law enforcement purposes.[66] The law regarding the interception of data and communications has been described as representing "a careful balance between the needs of law enforcement authorities to detect crime on the one hand and the expectations of privacy on the part of individuals on the other hand".[67]

4.35 Privacy was expressly acknowledged in the tracking device regime in sections 200A to 200P of the Summary Proceedings Act 1957. To issue a tracking device warrant, the judge hearing the application must be satisfied that there is a public interest in issuing the warrant, taking into account a number of factors, including the degree to which privacy or property rights are likely to be intruded upon.[68]

4.36 A further privacy dimension for searches and seizures by State agencies arises under section 21 of the New Zealand Bill of Rights Act 1990 (which protects the right to be secure against unreasonable search or seizure), discussed further below.

Human Rights Commission Act 1977

4.37 The Human Rights Commission Act 1977 signalled a more general concern about privacy. The Human Rights Commission was given functions in relation to privacy which included inquiring generally into any matter or any technical development if it appeared to the Commission that the privacy of the individual was being infringed thereby. It could report to the Prime Minister matters of concern about privacy, invite representations from members of the public, and make public statements in relation to any matter affecting the privacy of the individual or any class of individuals. The functions of the Commission in this regard were not of an enforcement nature. They could more accurately be described as monitoring or overview functions.[69]

---

62 The definition of "interception device" in the Crimes Act 1961, s 216A(1), was introduced by the Crimes Amendment Act 2003.

63 Hon Bruce Robertson (ed) Adams on Criminal Law (loose leaf, Brookers, Wellington, Crimes Act 1961, 1992) para CA 216A.03 (last updated 19 October 2007).

64 Crimes Act 1961, s 216B(2)(a).

65 Sections 248 to 254 in Part 10 of the Crimes Act 1961 (Crimes involving Computers) were introduced by the Crimes Amendment Act 2003. However, it is worth noting that privacy is not the sole policy concern behind these provisions. See BW Napier "An End to Hacking?" [1989] 133 Solicitor's Journal 1554, commenting on the report of the United Kingdom Law Commission *Criminal Law: Computer Misuse* (London, Her Majesty's Stationery Office, 1989): "it is not the invasion of privacy or the breach of confidentiality that is of most concern. The worst danger lies in the threat which unauthorised access poses to the integrity of systems, and the public's confidence in such integrity."

66 Part 11A Crimes Act in relation to the use of interception warrants; s 252(3) in relation to access to a computer system.

67 David Harvey *internet.law.nz* (2 ed, LexisNexis, Wellington, 2005) para 4.7. See also *Moulton v Police* [1980] 1 NZLR 443 (CA) as to the balance between order and freedom in the granting of police powers.

68 Summary Proceedings Act 1957, s 200B.

69 Human Rights Commission Act 1977, s 67. The Human Rights Commission Act 1977 was repealed and replaced by the Human Rights Act 1993 and these functions were transferred to the Privacy Commissioner under the Privacy Act 1993.

Official Information Act 1982

4.38 The Official Information Act 1982 was a milestone in freedom of information in New Zealand.[70] It provided for the first time that information held by governmental agencies was to be generally available to the public, but there were exceptions. For present purposes the most significant was "the privacy of natural persons". The Act's balance between freedom of information and privacy is reflected in its long title. The long title reads:

> An Act to make official information more freely available, to provide for proper access by each person to official information relating to that person, to protect official information to the extent consistent with the public interest and the preservation of personal privacy, to establish procedures for the achievement of those purposes, and to repeal the Official Secrets Act 1951.

4.39 Among the purposes of the Act is: "To protect official information to the extent consistent with the public interest and the preservation of personal privacy."[71]

4.40 It is important to note that personal privacy is not a conclusive reason for withholding information under the Act. Even when that ground is made out, a balancing exercise must still be carried out to see whether the public interest in the information outweighs the privacy interest.[72] That is significant. The acknowledgment that privacy is not an absolute value is consonant with other developments. Both the Broadcasting Standards Authority, in its jurisdiction under the Broadcasting Act 1989, and the courts have acknowledged that privacy rights can be outweighed by the public interest in receiving information, discussed further below.[73]

Privacy Act 1993

4.41 The Privacy Act 1993 was passed to promote and protect individual privacy in general accordance with the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[74]

4.42 The Act was a major initiative aimed at giving substantial protection to informational privacy; its Information Privacy Principles establish a framework for limiting the use and disclosure of personal information.[75] For example, where personal information is collected from a person (IPP 3), these limits are established by the collecting agency's declared purpose, subject to certain exceptions in IPP 10 and IPP 11.

---

70 In relation to official information held by local authorities, see the Local Government Official Information and Meetings Act 1987.

71 Official Information Act 1982, s 4(1)(c).

72 Official Information Act 1982, s 9(2)(a).

73 For discussion of the relationship between the Privacy Act 1993 and the Official Information Act 1982, see John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, Auckland, 2005) 277-278.

74 New Zealand adopted the OECD Guidelines on 23 September 1980: P Roth Privacy Law and Practice (loose leaf, LexisNexis, Wellington, International Developments, 2007) commentary ITL 1.3(a). These Guidelines are discussed further in chapter 7 below.

75 For the history leading up to enactment of the Privacy Act 1993, see Longworth and McBride, above n 57, ch 3.

4.43 The strength of the Privacy Act 1993 is in regulating the collection and storage of personal information by government departments, agencies such as hospitals and universities, and private-sector bodies. Of course, the application of the Act is subject to any other specific legislation that may, for example, expressly authorise the collection of personal information other than in accordance with the Privacy Act's Information Privacy Principles.

4.44 The Privacy Act 1993 is by far the most significant New Zealand Act about privacy. It will be the subject of separate study as part of the Commission's Review of Privacy, but in the context of the present discussion the following points may be made about it.

4.45 First, the Act takes a broad view of privacy in relation to personal data protection but does not deal at all with other aspects of privacy, such as local privacy. In relation to personal data protection, it goes well beyond protection against disclosure of private information and against surveillance. The Act lays down principles relating to:

- the collection of personal information;
- the storage and security of personal information;
- access by an individual to information held about him or her;
- the accuracy of personal information held by an agency;
- limits on the use of personal information; and
- limits on the disclosure of personal information.

4.46 Second, the Act is concerned with "personal information" about an identifiable individual, defined as "a natural person, other than a deceased natural person". Section 2 of the Act provides that personal information means:

> information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, and Marriages Registration Act 1995 or any former Act.

The definition of that term[76] goes wider than what many people would regard as "private" facts, such as "information relating to health, personal relationships, or finances".[77]

4.47 Third, the Act's privacy principles apply to information held by both public and private sector agencies. This can be contrasted with the Australian Privacy Act 1988 (Cth), which contains two sets of privacy principles: the eleven Information Privacy Principles that regulate Commonwealth Government agencies, and the ten National Privacy Principles that regulate private sector and health service providers.[78]

4.48 Fourth, the Act makes provision for "public registers" as that term is defined in the Act, and lays down certain principles relating to them, including, in particular, the principle that information obtained from public registers should not be aggregated for sale.[79]

---

76 The breadth of "personal information" under the Privacy Act 1993 is discussed in *Harder v Proceedings Commissioner* [2000] 3 NZLR 80, para 24 (CA) Tipping J and para 49 Gault J.

77 *Australian Broadcasting Commission v Lenah Game Meats* (2001) 208 CLR 199, para 42 Gleeson CJ. See also the discussion of "private facts" in paras 3.16-3.19.

78 Doyle and Bagaric, above n 22, 117.

79 Privacy Act 1993, s 59, Public Register Privacy Principle 2.

4.49 Fifth, the Privacy Act 1993 does not mandate the balancing of privacy against the public interest that can be seen in other legal contexts.[80] Rather, some of the privacy principles it lays down are subject to a number of detailed exceptions. Some of those exceptions (for example, threats to health and safety, or prejudice to the maintenance of the law) are, no doubt, aspects of the public interest, but the lists of exceptions, different for each principle, are not exactly coincident with public interest.

4.50 Sixth, the privacy principles set out in the Act are not enforceable in a court of law.[81] Infringement of them can be the subject of a complaint to the Privacy Commissioner, and in some cases the matter may be taken further to the Human Rights Review Tribunal, which does have power to award damages.

4.51 Seventh, the news media in their news activities are exempted from the Act's principles.[82]

4.52 Eighth, the information protection provisions of the Privacy Act go beyond the protection of autonomy and equality of respect, which we have isolated in chapter 3 as the values protected by privacy under the "core values" approach. The Act is in fact concerned to protect individuals against many potentially detrimental uses of their personal information. For example, it aims to control identity fraud and other criminal activity, and also to minimise the nuisance of direct marketing. The Act therefore can be seen as consistent with the harm-based approach developed by Daniel Solove, the second of the two options we identify in chapter 3 for classifying privacy.[83]

4.53 Finally, the Privacy Act 1993 is a key adequacy requirement for New Zealand to claim compliance with the European Data Protection Directive.[84] The Directive has considerable extra-territorial effect because it prohibits the export of personal data from within the European Union to countries that do not have an "adequate level of protection" for such data. Adequacy is judged within the European Commission which holds a "white list" of countries to which European states can export personal data. New Zealand's adequacy status is therefore important for industries with financial and trading links with Europe.[85]

---

80 However, the Privacy Act 1993, s 14(a), sets out a number of matters to which the Privacy Commissioner is to have regard in exercising powers under the Privacy Act, including "the protection of important human rights and social interests that compete with privacy." See also the Privacy Act, s 54(1), under which the Privacy Commissioner may authorise an agency to deal with personal information in breach of certain information privacy principles if satisfied, in the special circumstances of the case, that the public interest outweighs to a substantial degree the interference with privacy, or involves a clear benefit to the individual concerned that outweighs the interference with privacy.

81 Privacy Act 1993, s 11(2). However, s 11(1) provides that legally enforceable rights are conferred by principle 6 subclause (1) insofar as it relates to personal information held by a public sector agency.

82 Privacy Act 1993, s 2(1), definition of "agency", (b)(xiii). Broadcasters are subject to the privacy principles developed by the Broadcasting Standards Authority, and the press is (voluntarily) subject to a privacy principle administered by the Press Council, see further paras 8.61-8.64.

83 Solove's taxonomy includes harms such as disclosure, exposure, increased accessibility, blackmail, appropriation and distortion within the "information dissemination" category. Solove's "invasions" category is not limited to spatial incursions but includes spam, junk mail and telemarketing as invasive acts that disturb one's tranquillity or solitude (see para 3.28).

84 The Directive was issued in draft in 1992, passed in 1995 and came into effect in October 1998. See further paras 7.43-7.52.

85 Examples of sectors at risk if privacy standards are inadequate include credit, finance, health, travel and policing.

Public registers

4.54 Since the enactment of the Privacy Act 1993, a number of legislative provisions have sought to secure privacy protection for personal details on certain public registers. Various protective mechanisms are outlined in the Law Commission's issues paper on Public Registers. These include name and address restrictions, restrictions regarding sensitive information, limiting access to certain users, and penalties for abuse of the information obtained from a public register.[86] Different public registers have adopted different mechanisms or combinations of mechanisms.[87]

Privacy and broadcasters

4.55 The Broadcasting Act 1976 broke new ground in providing that the Broadcasting Corporation of New Zealand must be responsible for maintaining, in its programmes and their presentation, standards which would be generally acceptable to the community. Among other things it was required to have regard to "the privacy of the individual".[88] Complaints could be lodged by members of the public about breaches of this and other standards and, if dissatisfied with the Corporation's handling of such a complaint, the complaint could be referred to a Broadcasting Tribunal. The 1976 Act has now been replaced by the Broadcasting Act 1989. The privacy standard has been continued in that legislation and extended to all broadcasters, and complaints about its breach are now heard by the Broadcasting Standards Authority.[89]

4.56 The Broadcasting Act 1989 provides that all broadcasters, whether state or private, must maintain standards which are consistent with the privacy of the individual.[90] There is no civil liability for breaches of privacy under the Act[91] and so complaints are not heard in the courts but go before the Broadcasting Standards Authority. The BSA has power to award up to $5000 compensation in cases where it finds the standard to have been breached.[92] In this Act, the Legislature took an innovative, and it might be thought, daring step. It took a concept which many have believed defies definition, accorded it legal consequences and conferred on a statutory tribunal of four members the task of defining and applying it. The Authority, rather than adopting a lay person's approach to the subject, from the outset formulated a set of principles to be applied to privacy complaints, deriving them largely from United States law.[93] Aspects of the principles are discussed in chapter 8, which also contains general discussion of privacy and the media.[94]

---

86 New Zealand Law Commission *Public Registers*, above n 20, 79 and following.

87 See John Edwards "Public Registers and Privacy" [2007] NZLJ 146 for examples of different privacy protective mechanisms for public registers since 1993, including the Domestic Violence Act 1995, the Transport (Vehicle and Driver Registration and Licensing) Act 1986, the Local Government (Rating) Act 2002, the Building Act 2004 and the Births, Deaths, Marriages and Relationships Registration Amendment Bill 2007.

88 Broadcasting Act 1976, ss 24 and 96.

89 The news media are exempt from the Privacy Act in relation to their news activities: Privacy Act 1993, s 2(1), definition of "agency", (b)(xiii).

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

91 Broadcasting Act 1989, s 4.

92 Broadcasting Act 1989, s 13.

93 The principles have been through a number of iterations over the years. The current version was promulgated in 2006, and is found on the Authority's website, www.bsa.govt.nz.

94 See also *Hosking v Runting*, above n 17, paras 101-105 Gault P and Blanchard J; Burrows and Cheer, above n 73, 256-272.

Court reporting

4.57 It was not until the Family Proceedings Act 1980, when fault had been eradicated from dissolution of marriage, that it became the rule that dissolution cases were heard in closed court with no publication, unless by order of the court.[95] In 1985 legislation was passed providing that, as a rule, the victims of sex offences could give their evidence with the public excluded from the court.[96]

4.58 In criminal proceedings there is a judicial discretion to prohibit publication of identifying details.[97] Generally, strong considerations are required before the principle of open justice can be overridden.[98] Nevertheless, some judges are referring to privacy values in relation to suppression matters.[99] In civil proceedings, name suppression has been granted on privacy grounds.[100]

4.59 An aspect of court reporting relates to the balance to be struck between privacy and the freedom of the press when the media wishes to publicise material used in a criminal investigation or prosecution. The issue is dealt with under the Criminal Proceedings (Search of Court Records) Rules 1974. In *R v Mahanga*,[101] the Court of Appeal considered the judicial discretion to be exercised under the rules allowing the inspection of any document relating to a criminal proceeding. It concluded that this discretion is to be exercised by weighing the competing interests presented by any particular application, including the legitimate privacy concern of the accused person, in a balancing process.

4.60 A balancing exercise was also involved in *Jones v Television New Zealand*,[102] where the Court had the power to control publicity concerning a child under its guardianship. Given the importance of the freedom of the press, any restrictions on publication were to be limited to those necessary to give effect to the welfare of the child (the first and paramount consideration). It was found not to be in the child's best interests to screen a video of an interview with the child, because of the effect it would have on the child, including raising his public profile, which could be a burden on his reintegration into normal life, after being abducted by his grandfather.

---

95 Family Proceedings Act 1980, s 159.

96 Summary Proceedings Act 1957, s 185C; Crimes Act 1961, s 375A; Evidence Act 1908, s 23AA, added in 1985. The Criminal Justice Act 1985, s 139, prohibits the publication of the names of victims of sexual offences, along with the names of those accused or convicted of sexual offences in certain circumstances.

97 Criminal Justice Act 1985, s 140.

98 For example, in *Re Victim X* [2003] 3 NZLR 220 (CA), the victim's desire for privacy was not a sufficiently strong consideration to justify granting name suppression for a potential kidnap victim (cited in Butler & Butler, above n 2, para 13.12.4.)

99 See for example, decisions of Baragwanath J in *X v Police* (10 August 2006) HC AK CRI-2006-404-259; *J v Serious Fraud Office* (10 October 2001) HC AK A126/01.

100 *Patient A v Health Board and Another* (15 March 2005) HC BLE CIV 2003-406-14 Baragwanath J (cited in Butler & Butler, above n 2, para 13.12.8).

101 *R v Mahanga* [2001] 1 NZLR 641, para 32 (CA). See also *R v Wharewaka* (2005) 21 CRNZ 1008 (HC); *Rogers v Television New Zealand Ltd* (2005) 22 CRNZ 668 (HC); *Television New Zealand v Rogers* [2007] 1 NZLR 156 (CA); *Rogers v Television New Zealand* [2007] NZSC 91.

102 *Jones v Television New Zealand* (21 November 2006) HC HAM CIV 2006-419-1616 Lang J.

Common law

4.61 As noted above, traditionally the common law did not recognise a right of privacy per se, and reliance had to be placed on some other tort or right of action that might incidentally provide a remedy for the privacy invasion. From the mid-1970s, the New Zealand courts have expressly acknowledged that the seriousness of the invasion of privacy was something to be taken into account in assessing damages in those other causes of action. Thus in *Ramsay v Cooke*,[103] a trespass case, there had been a repeated and deliberate crossing of the plaintiffs' land, the defendant acting in an arrogant manner. The plaintiffs were awarded aggravated damages of $2500. Holland J said they were "clearly entitled to damages because of their loss of privacy and their rights as land owners to keep others off."

4.62 There have been similar acknowledgements by the English courts of the significance of privacy in such cases. For example, in the case of *Bernstein v Skyviews & General Limited*,[104] while it was found that a landowner had no action in respect of an aircraft flying at a reasonable height above his land to take photographs, the court noted that it might be different if there had been repeated flyovers of that kind. As Griffiths J said:[105]

> But if the circumstances were such that the 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 for which they would give relief.

4.63 The dicta in some cases are far reaching, none more so than that of Lord Scarman in *Morris v Beardmore,* a case where a Police Officer had entered private property for the purposes of administering a breath test. Lord Scarman said: "I have deliberately used an adjective which has an unfamiliar ring to the ears of common lawyers. I have described the right to privacy as 'fundamental'."[106]

4.64 That the New Zealand courts became increasingly aware of privacy as a value is demonstrated also by their dicta when applying the legislation involving search or interception warrants.[107] For example, in *Auckland Medical Aid Trust v Taylor*,[108] 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.

103 *Ramsay v Cooke* [1984] 2 NZLR 680, 687 (HC).

104 *Bernstein v Skyviews & General Limited* [1978] QB 479.

105 Ibid, 489.

106 *Morris v Beardmore* [1981] AC 446, 464 (HL).

107 For example *R v Jefferies* [1994] 1 NZLR 290 (CA); *R v Fraser* [1997] 2 NZLR 442 (CA). See Burrows, above n 4, para 18.2.02.

108 *Auckland Medical Aid Trust v Taylor* [1975] 1 NZLR 728, 737 (CA).

4.65 And in *Transport Ministry v Payn*,[109] Woodhouse J, considering a traffic officer's power to enter private premises to administer a breath test, said:

> But this case involves far wider issues and I think, too, that something much more basic than private property rights are concerned. Rights of property in this context have the special significance that they enable individuals to maintain their right to privacy and their civil liberties in general and they underline the value attached to personal independence and freedom from official harassment.

4.66 In *Moulton v Police*,[110] the Court of Appeal gave consideration to the police power to obtain information necessary to identify an arrested person:[111]

> 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...

4.67 Since the enactment of the Broadcasting Act 1976 (now 1989) and the Privacy Act 1993, jurisdiction for breaches of privacy covered by those statutes lies with specialist tribunals, rather than with the courts. Decisions of these tribunals are not part of the common law, although decisions of the Broadcasting Standards Authority have influenced the courts in relation to the development of the privacy tort, the key common law development in this period culminating in the Court of Appeal decision in *Hosking v Runting*,[112] discussed below.

The development of a privacy tort

4.68 At the end of the 19th century, the American jurists Warren and Brandeis wrote one of the most influential legal articles of all time.[113] Using early English decisions in areas such as invasion of property rights, breach of confidence or trade secrets, defamation and copyright, they argued for a general right to be let alone and advocated that there should be a tort of invasion of privacy. It was their view that privacy should be a legal right, enforceable by action in the courts:[114]

> The argument, of course, was that the existing case-law already contained the ingredients which are necessary to make up a general concept of privacy, but the courts had not then seen the wood for the trees. Working inductively through a limited number of cases in the areas of contract and industrial property it was shown how damages for invasion of privacy were awarded parasitically. Existing nominate heads of liability were being used to protect incidental interests of privacy which, more logically, ought to be isolated from existing remedies and re-classified as a separate and independent head of liability.

109 *Transport Ministry v Payn* [1977] 2 NZLR 50, 64 (CA).

110 *Moulton v Police*, above n 67, 446.

111 Police Act 1958, s 57(1).

112 *Hosking v Runting,* above n 17.

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

114 Dworkin, above n 28, 419.

4.69 The American courts followed the lead of Warren and Brandeis and, aided by reference to the United States Constitution, established a privacy tort. Such was the open-endedness of the concept of privacy, however, that by 1960, after over 300 reported American cases on privacy,[115] William Prosser wrote in an almost-equally influential article that from the seeds sown by Warren and Brandeis there had in fact emerged four different torts.[116] They were publication of private facts; intrusion into solitude or seclusion; publication placing the plaintiff in a false light; and appropriation of image without consent. The case law in the United States is voluminous and not always consistent.

4.70 In the other common-law countries there was initially no taste for following the American lead. In England in particular, there were strong statements, which have continued even in recent times, that English law recognises no right to privacy.[117] That was so despite the sometimes provocative facts of the cases which came before the courts. In the best known of them,[118] a famous actor was held to have no redress in privacy when journalists entered his hospital room when he was recovering from brain surgery and attempted to interview and photograph him as he lapsed in and out of consciousness. The court expressed its outrage at what had happened, but said that English law provided no remedy for breaches of privacy. In 1996 Lord Hoffman reiterated in the House of Lords that "English common law does not know a general right of privacy."[119]

4.71 This growing attention to privacy, which is evident in both the judgments of the courts and Acts of Parliament, was bound to raise the question of whether New Zealand and the other common-law jurisdictions should eventually follow the lead of the United States courts.

4.72 Nevertheless, while English law has so far declined to treat invasion of privacy as a cause of action in itself, it has extended the boundaries of breach of confidence to allow 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.[120] The boundaries of the breach of confidence action have been further expanded under the influence of the Human Rights Act 1998 (UK).[121] In the leading case of *Campbell v MGN*,[122] the House of Lords allowed a well known celebrity model damages when a newspaper published details of drug therapy she was

115 Ibid, 420.

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

117 Suggestions that there should be a tort of offensive invasion of privacy were made by several textbook writers but went largely unheeded: TL Yang "Privacy: a Comparative Study of English and American Law" (1966) 15 ICLQ 175, 176. Megan Richardson suggests that the un-English nature of the rather Kantian premise of "inviolate personality" invoked by Warren and Brandeis helps explain why the English courts did not follow their theory: "Privacy and Precedent: the Court of Appeal's Decision in *Hosking v Runting*" (2005) NZBLQ 82, 84.

118 *Kaye v Robertson*, above n 27.

119 *R v Brown* [1996] AC 543, 557 (HL).

120 See 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.

121 *Douglas and others v Hello! Ltd* [2007] UKHL 21.

122 *Campbell v MGN* [2004] 2 AC 457 (HL). For discussion of *Campbell* and other English breach of confidence decisions, see *Hosking v Runting*, above n 17, paras 23-53 Gault P and Blanchard J; Burrows and Cheer, above n 73, 236-243; Burrows, above n 4, para 18.4.04; Moreham, above n 120.

undergoing, together with a photograph of her outside a rehabilitation centre.[123] Although the English courts have preferred to proceed on the traditional ground of breach of confidence, the term "privacy" occurs many times in the judgment.[124] 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:[125]

> 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.

4.73 The New Zealand courts have reached a similar position rather more directly. As early as 1985 it was said to be arguable that there existed a tort of publication of private facts.[126] That view gathered momentum until in 2004 the New Zealand Court of Appeal, by a majority of three to two, held that there is indeed such a tort in this country.[127]

4.74 This was the decision of the Court of Appeal in *Hosking v Runting*.[128] 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.

4.75 The majority of the Court of Appeal confirmed both the existence of the privacy tort for the publication of private facts, and that the tort did not provide a remedy to the Hoskings to prevent publication of the photographs taken of their children in a public street.[129]

---

123 Ms 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.

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

125 *Campbell v MGN*, above n 122, 465. See further as to the similarity between the breach of confidence doctrine and the privacy tort: Doyle and Bagaric, above n 22, 72; Andrew Geddis "Hosking v Runting: A Privacy Tort for New Zealand" (2005) 13 Tort L Rev 5, 7; *Wainwright v Home Office*, above n 21, 1145 Lord Hoffmann (quoting Sedley LJ in *Earl Spencer v United Kingdom* (1998) 25 EHRR CD 105).

126 *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716 (HC).

127 For discussion of the New Zealand decisions relating to the privacy tort, see *Hosking v Runting*, above n 17, paras 77-86 Gault P and Blanchard J; Burrows, above n 4, para 18.5; Burrows and Cheer, above n 73, 245-251; Rosemary Tobin, "Invasion of Privacy" [2000] NZLJ 216. For discussion of New Zealand privacy tort cases since *Hosking v Runting*, see "Hosking and Beyond", above n 124, 403-408.

128 *Hosking v Runting*, above n 17.

129 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).

4.76 The judgment of Gault P and Blanchard J defined the elements of the new tort:[130]

> 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 that there should be "a defence enabling publication to be justified by a legitimate public concern in the information."

4.77 The judgment raises a number of issues about the new tort. One important issue is the nature of the harms for which the tort should provide redress and the remedy available to a plaintiff who succeeds in establishing an invasion of privacy that falls within the parameters of the tort. The judgment identifies the harm to be protected against as "in the nature of humiliation and distress,"[131] with damages awards as the main redress, and injunctive relief only in particular cases.[132] Awards of damages for mental distress are a relatively new phenomenon and as yet there is no clear benchmark for quantifying them. It is also unclear how far the tort will redress other potential harms, such as reputational damage, financial loss and inconvenience (for example, arising from a disclosure that results in identity theft or fraud), or disclosures that give rise to physical damage or threats to personal safety.

4.78 So far, judicial development of the tort extends only to publication of private facts and therefore protects informational privacy interests only. Generally speaking, the tort does not extend to a cause of action in privacy based upon the publication of photographs taken in a public place, but there could be exceptional cases.[133] It has been left open whether our courts may be inclined also to extend it, as the American courts have done, to intrusion into solitude or seclusion: in other words whether they will be prepared to hold that surveillance or other privacy intrusions may in some circumstances be tortious also.[134] The development of the new tort will be considered at a later stage of the Commission's Review of Privacy.

4.79 Other Commonwealth jurisdictions have not gone so far in recognising a tort of privacy. In some of the Canadian provinces there are statutory torts, but in those where there are not, the common-law courts appear not to have reached a clear position.[135] The same is true in Australia, the High Court having left open the question of whether a tort exists and the lower courts subsequently arriving at inconsistent decisions.[136]

---

130 *Hosking v Runting*, above n 17, 32.

131 Ibid, para 128 Gault P and Blanchard J.

132 Ibid, paras 149, 158 Gault P and Blanchard J; para 258 Tipping J.

133 See, for example, *Peck v United Kingdom* [2003] ECHR 44647/98, concerning the disclosure to the media of CCTV footage by a local authority of the appellant in a public street brandishing a knife with which he had attempted to commit suicide; *Von Hannover v Germany* [2004] EMLR 21, concerning the publication of paparazzi photographs of Princess Caroline of Monaco in German magazines; and *Campbell v MGN*, above n 122.

134 Their Honours expressly left this question open in *Hosking v Runting*, above n 17, para 118 Gault P and Blanchard J.

135 For discussion of the position in Canada, see *Hosking v Runting*, above n 17, paras 60-65 Gault P and Blanchard J.

136 Burrows and Cheer, above n 73, 244. See also *Hosking v Runting*, above n 17, paras 54-59 Gault P and Blanchard J.

PRIVACY AND HUMAN RIGHTS: THE IMPACT OF THE NEW ZEALAND BILL OF RIGHTS ACT 1990

4.80 The affirmation of human rights in the New Zealand Bill of Rights Act 1990 has been influential in establishing a human rights framework. Certain human rights are connected to or supported by privacy, such as freedom of expression,[137] freedom from discrimination[138] and freedom from unreasonable search and seizure.[139] The Canadian Privacy Commissioner has argued that "Our fundamental rights and freedoms – of thought, belief, expression and association – depend in part upon a meaningful measure of individual privacy."[140]

4.81 As noted by John Burrows:[141]

> Our jurisprudence is becoming more rights-based. That movement is international, and is evidenced in New Zealand in particular by the New Zealand Bill of Rights Act 1990. Although our Bill of Rights Act does not specifically codify a right of privacy, it has sensitised us to the essential dignity of the individual. There has been writing internationally of privacy as a fundamental human right.

4.82 The importance of the dignity of the individual has been acknowledged by members of the judiciary. In *R v Brooker,* Thomas J emphasised that dignity and worth of the person is the key value underlying the rights affirmed in the New Zealand Bill of Rights Act 1990.[142] Of all these rights:[143]

> Probably none are more basic to human dignity than privacy. It is within a person's sphere of privacy that the person nurtures his or her autonomy and shapes his or her individual identity. The nexus between human dignity and privacy is particularly close, including the link between a person's dignity and the sanctity of his or her home where their privacy is nurtured.

4.83 In *R v Wharewaka*, Baragwanath J, quoting from English authority, said that recent developments reflected "a general appreciation that the dignity of the individual is a core value, indeed the fundamental value, of a civilised society".[144]

4.84 And in *Hosking v Runting*, Tipping J said:[145]

> It is of the essence of the dignity and personal autonomy and wellbeing of all human beings that some aspects of their lives should be able to remain private if they so wish.

4.85 Such judicial statements strike a chord with the core values of autonomy and equality of respect underlying privacy, discussed in chapter 3. Commenting on this sort of language in *Hosking*, Megan Richardson notes:[146]

137 For discussion of the relationship between privacy and freedom of information, see paras 8.7-8.15.

138 See Rishworth and others, above n 2, 359.

139 See paras 4.98-4.104 below.

140 The Canadian Privacy Commissioner *Genetic Testing and Privacy* (Ottawa, 1995) 2. See also para 2.48, as to the political and social value of privacy.

141 Burrows, above n 4, 18.3.

142 *R v Brooker* [2007] NZSC 30, para 182 Thomas J.

143 Ibid.

144 *R v Wharewaka*, above n 101, para 26 Baragwanath J.

145 *Hosking v Runting*, above n 17, para 239 Tipping J.

146 Richardson, above n 117, 93.

parallels in recent privacy-breach of confidence cases in which such references are made alongside the individual flourishing and social progress rhetoric of liberal utilitarianism. Might these perhaps indicate that both doctrines [the tort of invasion of privacy and breach of confidence] are becoming more imbued with a Kantian ideal of inviolate personality; that utilitarian thinking is becoming relatively less significant in an era of human rights discourse? More likely, I suggest, what is now emerging is an idea of dignity as another interest to be weighed in the utilitarian balance – ie respect for the individual, and trust that such respect will be accorded, is coming to be understood as an important, albeit not inviolable, feature of modern liberal welfare society (probably, if more closely analysed, a key attribute of individual flourishing and social progress). This is a logical utilitarian approach to dignitary values, and not just because more of those whose welfare is being considered might now claim to care about their dignity than before: it *is* important in a basic utilitarian sense, as those who have experienced both its recognition and its loss are particularly well placed to appreciate.

4.86 The passing of the Privacy Act 1993 has also been influential on attitudes to privacy as a signal that New Zealand takes privacy seriously.

4.87 Nevertheless, there is no express constitutional guarantee of the right to privacy in New Zealand. Although 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", the Act does not include a statement of the general right to privacy contained in Article 17 of the ICCPR:

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.

4.88 A right to privacy is included in Article 8 of the European Convention on Human Rights, incorporated into the law of the United Kingdom through the Human Rights Act 1998.[147] A right to privacy is expressly mentioned in the Charter of Human Rights and Responsibilities Act 2006 (Vic) and the Human Rights Act 2004 (ACT). In the United States, there is no explicit right to privacy in the Constitution but there is a limited constitutional right to privacy based on a number of provisions in the Bill of Rights.[148] Similarly, the Canadian Charter of Rights and Freedoms does not specifically guarantee a right to privacy. However, in interpreting section 8 of the Charter (the right to be secure against unreasonable search and seizure), Canada's courts have recognised an individual's right to a reasonable expectation of privacy.[149]

4.89 Privacy is not an express right under the New Zealand Bill of Rights Act 1990. Under section 28, an existing right or freedom is not abrogated or restricted because it is not included or not fully included. However, any Bill of Rights analysis under section 5 (justified limitations), section 6 (interpretation consistent with Bill of Rights to be preferred) or section 7 (Attorney-General to

147 Human Rights Act 1998 (UK), s 1(1), Schedule 1.

148 *Privacy & Human Rights: An International Survey of Privacy Laws and Developments* (Electronic Privacy Information Center, Washington, DC, 2001) 310.

149 Ibid, 110.

report to Parliament where Bill appears to be inconsistent with Bill of Rights) is to be performed with respect to the rights and freedoms *contained* in the Bill of Rights. This suggests that rights and freedoms expressly contained in the New Zealand Bill of Rights Act 1990 have a different status than rights and freedoms that are excluded, notwithstanding section 28. This conclusion is also supported by Paul Rishworth:[150]

> It also goes without saying that the recognition of other rights in s. 28 does not mean that those other rights are to be treated as if they are *affirmed* by the Bill of Rights. The point of the Bill of Rights is to affirm the rights it affirms, while recognising in s. 28 that there are other rights that it has not affirmed.

4.90 However, notwithstanding the unaffirmed status of privacy, considerations of privacy potentially arise in certain New Zealand Bill of Rights Act enquiries:

- under section 5 (as a justifiable limitation on affirmed rights and freedoms); and
- under section 21 (protection from unreasonable search and seizure by State enforcement agencies).

Privacy as a justifiable limitation on freedom of expression: two case examples

4.91 The potential for the courts to censure privacy intrusions in performing a balancing of competing rights under section 5 the New Zealand Bill of Rights Act 1990, was the matter of judicial debate in *Brooker v Police*.[151] The Supreme Court considered whether a protest unduly impacted on the local 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.[152] The appeal concerned the meaning of "behaves in [a] disorderly manner" under section 4(1)(a) of the Summary Offences Act 1981.

4.92 The Supreme Court was divided 3:2. 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:[153]

> 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.

4.93 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,[154] and considered that it was necessary to balance the conflicting rights.

---

150 Rishworth and others, above n 2, 67.

151 *Brooker v Police*, above n 142.

152 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.

153 *Brooker v Police*, above n 142, para 40 Elias J.

154 Ibid, para 129 McGrath J.

4.94 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:[155]

> 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.

4.95 The decision in *Brooker* can be contrasted with the majority decision of the Court of Appeal in *Hosking v Runting* (3:2) that the tort of invasion of privacy is a reasonable limit on free expression in terms of section 5 of the Bill of Rights Act in certain circumstances involving the publication of private facts.[156] Gault P and Blanchard J did not accept that "omission from the Bill of Rights Act can be taken as legislative rejection of privacy as an internationally recognised fundamental value".[157] The question as their Honours saw it was how the law should reconcile the competing values.[158] Tipping J concluded that in certain circumstances, privacy values could outweigh the right to freedom of expression:[159]

> When privacy values are found to outweigh the right to freedom of expression, and the law recognises that by placing a limitation on freedom of expression, that limitation will, in terms of s 5 of the Bill of Rights, be a limit prescribed by law. It will also be a limit which is reasonable and demonstrably justified in a free and democratic society.

4.96 However, the minority did not accept that privacy could be a justifiable limitation on free speech in terms of section 5 of the New Zealand Bill of Rights Act 1990. Anderson J considered that privacy is in the nature of a value only (the choice that an ordinary person wishes to exercise in respect of the incidence and degree of social isolation or interaction) which should not trump the right of freedom of expression.[160] Keith J considered that the proposed tort was not demonstrably justified as a limitation on freedom of expression.[161]

4.97 The nature of the balancing exercise was also considered by Baragwanath J in *R v Wharewaka*, a case involving an application by Television New Zealand to obtain video footage used in a criminal proceeding under the Criminal Proceedings (Search of Court Records) Rules 1974:[162]

---

155 Ibid, para 164 Thomas J; see also para 285.

156 Although the privacy tort may not directly engage the New Zealand Bill of Rights Act where private parties are involved, the decision of the majority assumes that the Act should have horizontal effect in this context.

157 *Hosking v Runting*, above n 17, para 92 Gault P and Blanchard J.

158 Ibid, para 116 Gault P and Blanchard J.

159 Ibid, para 237 Tipping J.

160 Ibid, paras 264-265 Anderson J; Burrows and Cheer, above n 73, 250.

161 Ibid, para 222 Keith J.

162 *R v Wharewaka*, above n 101, para 27 Baragwanath J.

> Neither freedom of expression nor privacy is an absolute right. Such non-absolute "rights", which it is the Court's function to balance, may usefully be seen as public interests to be meshed appropriately with other public interests – whether they are to be found in the Bill of Rights, the Human Rights Act or in the principles of common law. Each is of such importance that where they conflict the balance between them must be struck in a carefully nuanced way.

While noting the different position of privacy under English and New Zealand law in constitutional terms, Baragwanath J considered that allowing privacy to be weighed in the balancing exercise was consistent with the decision of the Court of Appeal in *R v Mahanga*.[163]

Section 21: search and seizure and reasonable expectations of privacy

4.98 The other circumstance in which privacy considerations potentially arise in relation to the New Zealand Bill of Rights Act 1990, is under section 21, which provides: "Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise."

4.99 The Court of Appeal has referred to the touchstone in section 21 being "the protection of reasonable expectations of privacy."[164] The reasonable expectation of privacy concept is not unique to New Zealand. Section 8 of the Canadian Charter of Rights and Freedoms is similar to section 21 of the New Zealand Bill of Rights Act 1990. The concept is also used in the United States for purposes of determining what is an unreasonable search under the Fourth Amendment to the Constitution.[165] The Fourth Amendment is usually seen as the codification of the English common law as expressed in *Entick v Carrington*.[166]

4.100 The protection of reasonable expectations of privacy under section 21 is by no means absolute. Rather, it is limited to unreasonable searches where the strength of the privacy interest outweighs other competing interests in the use of evidence obtained from the search. Section 21 permits searches which are reasonable to interfere with reasonable expectations of privacy, and even where the search is unreasonable, other competing factors may outweigh the privacy interest involved. Section 21 also involves a grading of privacy interests largely, but not solely, based on proprietorial connections to the property being searched.[167]

4.101 General propositions about the relationship between unreasonableness and privacy were set out in by the Court of Appeal in *R v Grayson & Taylor*.[168]

---

163 *R v Mahanga*, above n 101.

164 *R v Fraser*, above n 107, 449. Privacy is not the only rationale however; section 21 reflects an amalgam of values, namely, property, personal freedom, privacy and dignity: see *R v Jefferies*, above n 107, 302 Richardson J.

165 Protection of privacy was first mentioned in relation to the Fourth Amendment in *Wolf v Colorado* (1949) 338 US 25 (cited in Flitton and Palmer, above n 7, 154).

166 *Entick v Carrington* (1765) 19 State Tr 1029: "By the laws of England, every invasion of private property be it ever so minute is a trespass." See Flitton and Palmer, above n 7, 155.

167 See further, New Zealand Law Commission *Search and Surveillance* (NZLC R97, Wellington, 2007) ch 2, for discussion of the concept of reasonable expectations of privacy under section 21, and ch 11 for discussion of the operation of section 21 in relation to surveillance.

168 *R v Grayson & Taylor* [1997] 1 NZLR 399 (CA). For a critique of this and other Court of Appeal decisions involving section 21, see Hart Schwartz "The Short Happy Life and the Tragic Death of the New Zealand Bill of Rights Act" [1998] NZ Law Rev 259. Section 21 protects corporate bodies as well as individuals, as confirmed in *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780, 790 (CA).

In *R v Williams*,[169] the Court of Appeal comprehensively reviewed the way in which section 21 should be applied. Section 21 determinations involve a two-stage process with privacy interests being relevant at both stages. For stage 1 to be met, there needs to be unreasonableness and a breach of a privacy interest.[170]

4.102 Stage 2 is then a balancing exercise to assess whether exclusion of the evidence is a balanced and proportionate response to the circumstances of the breach.[171] The first step in this balancing stage is synthesising the extent of the illegality and the nature or strength of the privacy interest in order to assess the overall seriousness of the breach.[172] In terms of the strength of the privacy interest, the Court observed:[173]

> The highest expectation of privacy relates to searches of the person and particularly intimate searches, such as strip searches (as in *Pratt*) or invasive procedures, such as DNA testing (as in *Shaheed*). In terms of searches of property, residential property will have the highest expectation of privacy attached to it…There will be some gradation even within a residential property however. The public areas will invoke a lesser expectation of privacy than the private areas of the house… Inaccessible areas such as drawers and cupboards (particularly ones where one would expect to find private correspondence or intimate clothing) would count as private areas. There will be less privacy expected in the garden, particularly in the front garden. The same applies to garages or outbuildings. There is also a lesser expectation of privacy in vehicles…, in commercial premises…., and on farmland, apart from the areas around the farm residences…

4.103 In a search of property, the connection of the person claiming a privacy interest is also important:[174]

> Given that the purpose of the exclusion of evidence under the Bill of Rights is to vindicate individual rights, the strength of the privacy interest of the individual involved will be of major significance. This will be judged by the degree of connection to the premises or land involved or to the property searched or seized in those premises. Obviously the person with a bare licence, whether or not they are present at the search, will have a lesser expectation of privacy than a person who is the owner or exclusive occupier of the premises or land.

4.104 The next step is to balance the breach against the public interest factors pointing away from the exclusion of the evidence.[175] The fact that there has been a breach of a "quasi-constitutional right," and the seriousness of the breach in question, must be given due weight.[176]

---

169 *R v Williams* (2007) 23 CRNZ 1 (CA).

170 For the Court's survey of possible grounds for unreasonableness, see ibid, para 24.

171 The balancing exercise was enunciated in *R v Shaheed* [2002] 2 NZLR 377 (CA), now reproduced in large part in section 30 of the Evidence Act 2006.

172 *R v Williams,* above n 169, para 115 William Young P and Glazebrook J. The court emphasized that these gradations are not meant to be rigid classifications.

173 Ibid, para 113 William Young P and Glazebrook J.

174 Ibid, para 124 William Young P and Glazebrook J.

175 Ibid, para 250 William Young P and Glazebrook J.

176 Ibid, para 251 William Young P and Glazebrook J.

ISSUES FOR FURTHER CONSIDERATION

4.105 Surveying the current landscape of privacy protection in *Hosking v Runting*, Keith J found legislative privacy protection to be of limited specific focus. His Honour described the varieties of planting in this landscape, "some of it very dense and deliberate, and its contrasting bare plains". He summarised the situation in these terms:[177]

> The many existing protections of privacy interests against the exercise of freedom of expression incorporate a range of variables: they may relate to face to face encounters or less direct ones; they may be limited to one on one encounters or cover communication to wider groups; they may be limited to expression or extend beyond it; they may simply prohibit the release of private information or they may also require a judgment to be made about the impact of the release; they may apply to particular categories of persons who exercise freedom of expression and not to others (who may indeed be explicitly excluded); they may specifically respond to particular technologies; they may mention privacy explicitly or they may not; they may be elaborated by international agencies, legislatures or courts or by the relevant profession, industry or occupational group; they may be supported by criminal, civil, disciplinary or other sanctions, in the ordinary courts, special tribunals, disciplinary bodies, or self-regulatory bodies; or the protection may come solely from the personal or professional assessment of the individual or organisation concerned.

4.106 Summarising the characteristics of legislation protective of privacy, Keith J noted that much of the law is particular:[178]

- The law is often responding to new technology, to new or newly-perceived situations, or to changing social conditions and attitudes.
- There is a choice between control over the release of information and requiring a judgement of consequence.
- Choices are made between legislation and self-regulation. Within the legislative responses, there are choices between criminal or civil liability (or both), or liability through special tribunals and disciplinary processes.

His Honour noted the legislative choice made in relation to the privacy and broadcasting statutes in particular, by leaving privacy to be developed and stated in codes or opinions by expert bodies and then applied to particular cases, in preference to allowing a right of action in the general courts.[179]

4.107 The current legislative landscape raises questions for a review of privacy law. Is the "particularity" approach to different aspects of privacy the best approach? Does it create undue complexity? Are there significant privacy gaps between particular statutory provisions?

4.108 To what extent can privacy be said to be a right? In 1985, the White Paper commentary in relation to clause 19 (enacted as section 21) of the proposed Bill of Rights stated:[180]

177 *Hosking v Runting*, above n 17, para 185 Keith J.

178 Ibid, para 203 Keith J.

179 Ibid, para 205 Keith J.

180 *A Bill of Rights for New Zealand: A White Paper* (Department of Justice, Wellington, 1985) 103-104. According to Gault P in *Hosking v Runting*, above n 17, para 93, the White Paper shows that Parliament was not concerned to entrench a vague and uncertain privacy right in the current New Zealand social climate.

> Freedom from unreasonable search and seizure is an aspect of the privacy of the individual. The Bill (like the Canadian charter) gives no general guarantee of privacy. 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.

4.109 Since the position enunciated in the White Paper, there have been important developments recognising various aspects of informational privacy, including the enactment of the Privacy Act 1993 and influential judgments of New Zealand's higher courts, including the decision of the Court of Appeal in *Hosking v Runting*.[181] The question is whether independent developments in relation to various aspects of privacy have culminated in what can now be said to be a general right of privacy, whether there is a group of independent but related privacy rights, or whether there is a mixture of various privacy interests, some of which may have achieved the status of rights.

4.110 There are clearly a number of specific privacy rights; however, a general right of privacy has only been enunciated at the level of international law. Rights in relation to informational privacy are protected by the Privacy Act, the Broadcasting Act, and the Court of Appeal's affirmation of the privacy tort. Local privacy is protected indirectly through various specific statutory offences and common law causes of action. Is this the best approach?

4.111 The Law Commission proposes to consider these questions in the following stages of the Privacy Review.

181 *Hosking v Runting*, above n 17.

Chapter 5:
Social Attitudes

5.1 Attitudes to privacy do not exist in a vacuum: they are shaped by history and culture, and by personal experiences. Consequently, they vary widely across historical periods and cultures, and between different individuals and social groups. This chapter provides some important context for the Commission's Review by exploring past and present attitudes to privacy, and the implications of these attitudes for law and policy.

5.2 We begin by considering the history of privacy in Western societies, and the development of the concept of privacy that is reflected in the "privacy paradigm" discussed in chapter 2. Other cultures have their own histories and perspectives on privacy, and we discuss privacy and culture in general before focusing specifically on Māori cultural perspectives. We then consider whether young people are growing up with different views of privacy from those of previous generations. One of the lessons of the history of privacy is that it is closely connected with technological change, and the networked world in which young people are growing up today has important implications for their understanding of privacy. We look at the use of public opinion poll data in studying privacy, and at what opinion polls reveal about New Zealanders' views of privacy, before concluding with some thoughts on the implications for law reform.

PRIVACY IN WESTERN SOCIETIES: A HISTORICAL PERSPECTIVE

5.3 There has been relatively little study of the history of privacy, and we are not aware of any historical research on privacy in New Zealand.[1] Nevertheless, we think it is important to provide some historical context for present-day debates about privacy. Our discussion is limited to the history of privacy in Europe and

1 Relevant works on the history of privacy in the US and Europe include David Flaherty *Privacy in Colonial New England* (University Press of Virginia, Charlottesville (VA), 1972); Richard Sennett *The Fall of Public Man* (Cambridge University Press, Cambridge, 1976); David J Seipp *The Right to Privacy in American History* (Program on Information Resources Policy, Harvard University, Cambridge (Mass), 1978); Barrington Moore, Jr *Privacy: Studies in Social and Cultural History* (M E Sharpe, Armonk (NY), 1984); Philippe Ariès and Georges Duby (gen eds) *A History of Private Life* (transl Arthur Goldhammer, 5 vols, Belknap Press, Cambridge (Mass), 1987-1991); Patricia Meyer Spacks *Privacy: Concealing the Eighteenth-Century Self* (University of Chicago Press, Chicago, 2003). For some short but useful historical overviews of the history of privacy, see Hannah Arendt *The Human Condition* (2 ed, University of Chicago Press, Chicago, 1958) 22-78; Edward Shils "Privacy: Its Constitution and Vicissitudes" (1966) 31 Law & Contemp Probs 281, 288-301; Alan F Westin *Privacy and Freedom* (Atheneum, New York, 1967) chs 1, 13; Raymond Williams "Private" in Raymond Williams *Keywords: A Vocabulary of Culture and Society* (Fontana/Croom Helm, London, 1976) 203-204; Ferdinand David Schoeman *Privacy and Social Freedom* (Cambridge University Press, Cambridge, 1992) ch 7; Perri 6 *The Future of Privacy* (vol 1, Demos, London, 1998) ch 1; Daniel J Solove "Conceptualizing Privacy" (2002) 90 Cal L Rev 1087, 1132-1140; James Q Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale LJ 1151, 1171-1189; "A Short History of Surveillance and Privacy in the United States" in National Research Council of the National Academies *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washington, DC, 2007) 349-365.

those societies in North America, Australia and New Zealand whose dominant cultural traditions have been inherited from Europe. We refer to these societies as "Western", although we recognise that this is a problematic term and that there are significant cultural differences between "Western" societies, including differences in concepts of privacy.[2] We discuss culture and privacy further below.

5.4 Examining the history of privacy helps us to understand that its meaning is not fixed, but changes over time. The way in which ideas about privacy have evolved may also provide some clues about how privacy may develop in future. Another reason for looking at the history of privacy is to provide some perspective on the widespread assumption that privacy is under unprecedented threat in today's world.[3] As Colin Bennett and Charles Raab observe, privacy is seen as "something 'we' once had; now it is something that public and private organizations employing the latest information and communications technologies are denying us."[4] A longer-term perspective, however, calls into question the extent to which "we" (or our ancestors) enjoyed privacy in the past.

5.5 The American novelist and essayist Jonathan Franzen writes that:[5]

> In 1890, an American typically lived in a small town under conditions of near-panoptical surveillance. Not only did his every purchase "register", but it registered in the eyes and the memory of shopkeepers who knew him, his parents, his wife, and his children. He couldn't so much as walk to the post office without having his movements tracked and analyzed by neighbors. Probably he grew up sleeping in the same bed with his siblings and possibly with his parents, too. Unless he was well off, his transportation – a train, a horse, his own two feet – either was communal or exposed him to the public eye.

Things were little different in the small towns and suburbs of New Zealand, even in relatively recent times.[6]

5.6 As Franzen points out, many people in earlier generations had little physical privacy. Neither was there a general expectation of privacy in personal communications until relatively recently. Letter-writing was not necessarily a private act in the 19th century and earlier. Those who were illiterate relied

2 Westin, above n 1, 26-30; Whitman, above n 1.

3 For example: "Today, more than ever before, we are witnessing the daily erosion of personal privacy and freedom" – Simson Garfinkel *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly, Sebastapol (Calif), 2000) 4; "Never in the history of humankind have we all been so spied upon" – Thane Burnett "Technology is Constantly Keeping Tabs on You" (15 April 2007) *The London Free Press* London (Canada) www.lfpress.com (accessed 18 April 2007).

4 Colin J Bennett and Charles D Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (2 ed, MIT Press, Cambridge (Mass), 2006) 7.

5 Jonathan Franzen *How to be Alone: Essays* (Fourth Estate, London, 2002) 47.

6 For example, Bill Pearson's essay "Fretful Sleepers" describes a New Zealand society in which people kept a close, and often disapproving, eye on their neighbours: Bill Pearson "Fretful Sleepers: A Sketch of New Zealand Behaviour and its Implications for the Artist", originally published in *Landfall* (1952), revised 1974, and reprinted in Russell Brown (ed) *Great New Zealand Argument: Ideas About Ourselves* (Activity Press, Grey Lynn, 2005) 47-96.

on others to write or read letters for them, and even where this was not the case letters were often read aloud or passed from person to person. Moreover, a legal right to privacy of correspondence, protecting letters from being opened by postal or other authorities without good cause, took some time to develop.[7] Even diaries and journals, now viewed as quintessentially private documents, were not necessarily considered private in the 19th century.[8] Telephone conversations, too, were far from private in the days when the operator could listen in on calls. It is worth noting, however, that while a general expectation of informational privacy may have developed relatively recently, the principle that information learned in the course of certain relationships (doctor/patient, lawyer/client, confessor/confessant) should be kept confidential is a much older one. It was in part by extending the concept of confidentiality that postal and telegraphic communication came to receive legal protection.[9]

5.7 If privacy is something "we" are in danger of losing as a result of technological and other developments (a question to which we will return later in this study paper), it is helpful to understand that the level of privacy we have come to expect has probably only existed for a few generations at most. That is not to say that these expectations of privacy are unreasonable or that privacy is not worth protecting. A historical perspective can, however, help to balance some of the more alarmist claims about contemporary erosion of privacy.

5.8 There are a number of other points to make about the history of privacy in the West that can usefully inform our understanding of privacy today.

5.9 First, the development of modern Western ideas of privacy is closely linked to the emergence of the concept of the self-contained individual. Historian Lynn Hunt argues that, from the 14th century onwards, individuals became more self-contained and their thresholds of shame lowered. Public urination and defecation, sharing food bowls and beds, and violent outbursts of emotion all became increasingly socially unacceptable and unpleasant. These developments "signaled the advent of the self-enclosed individual, whose boundaries had to be respected in social interaction."[10] Such ideas about individual boundaries are at the heart of Western notions of privacy. At the same time, the development of printing, followed by increasing literacy, also played an important role in forming concepts of individuality and privacy. Reading became a solitary activity, and one in which readers could learn about the world without revealing anything about themselves (in contrast to oral communication and, increasingly, to online communication today).[11]

---

7 Michelle Perrot (ed) *A History of Private Life* (transl Albert Goldhammer, vol 4, Belknap Press, Cambridge (Mass), 1990) 132, 453; David Fitzpatrick *Oceans of Consolation: Personal Accounts of Irish Migration to Australia* (Cornell University Press, Ithaca (NY), 1994) 476-478; Solove, above n 1, 1142-1143.

8 According to Margot Fry, some 19th-century diaries were private, but others were intended to be read by other people, or even to be published: Margot Fry *Tom's Letters: The Private World of Thomas King, Victorian Gentleman* (Victoria University Press, Wellington, 2001) 130.

9 Neil M Richards and Daniel J Solove "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Geo LJ 123, 133-145. The Hippocratic Oath, which states that doctors must not divulge information learned in the course of their professional service, dates from around 400 BC, while lawyer-client privilege dates back to at least 1577.

10 Lynn Hunt *Inventing Human Rights: A History* (W W Norton, New York, 2007) 82-83.

11 Felix Stalder "The Voiding of Privacy" 5, accessed at http://felix.openflows.com and published as "The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy" (2002) 7 Sociological Research Online www.socresonline.org.uk.

5.10 Second, in their historical development, local and informational privacy have been closely intertwined. It is very hard to keep information about yourself private when you are living at close quarters with others. From the 17th century onwards the home, and particular spaces within the home, became increasingly private. Gradually, people stopped living and working in the same building, and houses were partitioned into rooms with particular uses, including separate bedrooms and other rooms for children. Houses were divided into public and private spaces, with public rooms creating transitional spaces between the private world of the family and the wider world.[12] All of these developments, in turn, allowed people to read, write and talk in private, thereby keeping personal information hidden from the eyes and ears of others.

5.11 Third, over time privacy has been democratised.[13] It was initially associated with the rising middle class, who could afford to create the kind of privacy in the home that we have just described (unlike the poorer classes), and who did not have responsibilities that required them to be under the public gaze (unlike the aristocracy). In time, however, the upper class joined the middle class in their taste for privacy, and eventually many working class people were also able to afford homes in which they could lead a private life. Increased privacy came to be associated with progress and civilisation, and visitors commented favourably on the privacy enjoyed by workers in New Zealand.[14] Missionaries in New Zealand disapproved of the fact that Māori houses were not divided into separate rooms, and reformers like the young Āpirana Ngata looked forward to the day when communal living would be dissolved and Māori would "enjoy privacy in our homes".[15]

5.12 Fourth, the boundaries of the public and the private have shifted over time. As Daniel Solove explains, it is not simply a question of certain matters changing from being clearly public to private or vice versa:[16]

> Particular matters have long remained private but in different ways; they have been understood as private but because of different attributes; or they have been regarded as private for some people or groups but not for others. In other words, to say simply that something is public or private is to make a rather general claim; what it means for something to be private is the central question.

Solove illustrates the shifting boundaries of public and private by looking at three matters that are commonly considered to be at the heart of the private sphere: the family, the body and the home.[17] He shows that these have not always been

12 Witold Rybczynski *Home: The History of an Idea* (Viking, New York, 1986); Helen M Leach "The European House and Garden in New Zealand: A Case for Parallel Development" in Barbara Brookes (ed) *At Home in New Zealand: Houses, History, People* (Brigid Williams Books, Wellington, 2000) 73-88; Solove, above n 1, 1137-1140; Antoine Prost and Gérard Vincent (eds) *A History of Private Life* (vol 5, Belknap Press, Cambridge (Mass), 1991) 4.

13 Prost and Vincent, above n 12, 7.

14 Erik Olssen "Towards a New Society" in Geoffrey W Rice (ed) *The Oxford History of New Zealand* (2 ed, Oxford University Press, 1992) 274.

15 Lachy Paterson "Rēweti Kōhere's Model Village" (2007) 41 New Zealand Journal of History 26, 31-32 (quote at 31 is from A T Ngata "Māori Politics and Our Relation Thereto" in *Papers and Addresses Read Before the First Conference of the Te Aute College Students' Association, February 1897* [Gisborne, 1897] 33).

16 Solove, above n 1, 1132.

17 Ibid, 1132-1140.

viewed as private in the way we understand them to be today. For example, public exposure of the nude body, and performing certain bodily functions such as urination and defecation in front of others, appear to have become more unacceptable over time.

5.13 Fifth, since the late-19th century concerns about the loss of privacy have been closely linked with developments in technology. One of the chief concerns of Warren and Brandeis in their famous article on "The Right to Privacy" was with the threat to privacy posed by "[i]nstantaneous photographs" and "numerous mechanical devices", coupled with an intrusive press.[18] Cheap, portable cameras able to take "instantaneous" photographs (so that subjects did not have to sit still for several minutes to have their picture taken) allowed people to take and publish "candid" photographs without the subject's consent, while the telegraph made it possible to transmit information about a person immediately around the world. Warren and Brandeis were by no means the only writers to complain about the perceived intrusions on privacy made possible by such inventions in the late-19th and early-20th centuries.[19] There was another wave of concern about privacy in the 1960s and 1970s as a result mainly of concern about storage of personal information in "computer databanks".[20] The rise of the internet since the late 1990s has seen a third wave of technology-related privacy fears, which are examined in the next chapter.

5.14 A number of key points emerge from this brief survey of the history of privacy in the West:

- Ideas about privacy have developed and changed over time, and will no doubt continue to change.
- It is not necessarily the case that there was more privacy in the past, and in some respects there may have been less.
- Ideas about privacy are closely associated with technological and social change, whether it be the development of printing, changes in housing, or the invention of the portable camera and the rise of popular journalism. Comparable changes in the future are likely to lead to further changes in concepts of privacy, and in people's "reasonable expectations of privacy".

CULTURE AND PRIVACY

5.15 The Law Commission Act 1985 requires the Commission, in making its recommendations, to take into account "te ao Māori (the Māori dimension)" and to give consideration to "the multicultural character of New Zealand society".[21] Contemporary New Zealand is home to people from a wide range of

18 Samuel D Warren and Louis D Brandeis "The Right to Privacy" (1890) 4 Harv L Rev 193, 195.

19 Westin, above n 1, 338; Dorothy J Glancy "The Invention of the Right to Privacy" (1979) 21 Ariz L Rev 1, 7-9; Daniel J Solove *The Future of Reputation: Gossip, Rumour, and Privacy on the Internet* (Yale University Press, New Haven, 2007) 105-110.

20 See for example *The Computer and Invasion of Privacy: Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives, Eighty-Ninth Congress, Second Session, July 26, 27, and 28, 1966* (US Government Printing Office, Washington, DC, 1966; reprinted by Arno Press, New York, 1967); Arthur R Miller *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press, Ann Arbor, 1971); *Privacy and Computers: A Report of a Task Force Established Jointly by Department of Communications/Department of Justice* (Information Canada, Ottawa, 1972); Law Revision Commission (New Zealand) *Report of Sub-Committee on Computer Data Banks and Privacy* (1973); Paul Sieghart *Privacy and Computers* (Latimer, London, 1976).

21 Law Commission Act 1985, s 5(2)(a).

non-European cultural traditions,[22] and any review of the law in this area must consider the possible impact of cultural diversity on community attitudes to privacy. Unfortunately, there has been little research on this subject so far.[23]

5.16 Some degree of desire for privacy seems to be universal among human societies, and the need to maintain a minimum area of separate space from others is shared with non-human animals.[24] This broad commonality, however, tells us little about what privacy means in practice in particular societies. Any cross-cultural study of privacy must aim to look for similarities and resemblances in concepts and practices, while avoiding the imposition of a Western frame of understanding on other cultures. The mere fact that there is no word in a particular language that equates precisely to "privacy", for example, does not mean that speakers of that language have no concept that is equivalent to privacy. Concepts, practices and laws that bear some resemblance to the English word "privacy" can be found in the Jewish, Arab Muslim and Chinese traditions, among others.[25] In a number of cultures, concepts akin to privacy tend to be focused on protecting the reputation of the family, and are often closely related to ideas of the secret and/or the sacred.[26]

5.17 Among the matters that may vary between cultures are:

- what types of information are considered private;
- what types of places are considered private;
- how privacy is maintained (by laws, by codes of restraint and avoidance, by religious restrictions, and so on); and
- under what circumstances it is considered acceptable to intrude on privacy (as understood within the particular culture).

5.18 In light of such cultural variation, the question may arise as to whether cultural factors should be taken into account in assessing whether the test for a successful claim of interference with privacy, as set out by Gault P and Blanchard J in *Hosking v Runting*,[27] has been met. In particular, should the offensiveness of publicity given to private facts be considered in relation to "an objective reasonable person" of the same cultural background as the plaintiff?

---

22 In the 2006 census, 14.6 per cent of New Zealand residents identified as Māori, 9.2 per cent as Asian, 6.9 per cent as Pacific peoples, and 0.9 per cent as Middle Eastern, Latin American and African: Statistics New Zealand *QuickStats About Culture and Identity: 2006 Census*.

23 For an Australian study see Office of the Victorian Privacy Commissioner *Privacy in Diverse Victoria: Attitudes Towards Information Privacy among Selected Non-English Speaking Background and Indigenous Groups in Victoria* (Privacy Victoria, Melbourne, 2002).

24 Westin, above n 1, 8-22.

25 Jeffrey Rosen *The Unwanted Gaze: The Destruction of Privacy in America* (Random House, New York, 2000) 18-19; Julie Gruenbaum Fax "Jewish Tradition Says Safety Trumps Privacy When it Comes to Mental Health" (27 April 2007) *Jewish Journal* Los Angeles www.jewishjournal.com (accessed 27 April 2007); Fadwa El Guindi *Veil: Modesty, Privacy and Resistance* (Berg, Oxford, 1999) 82-96; Cao Jingchun "Protecting the Right to Privacy in China" (2005) 36 VUWLR 645; Bonnie S McDougall "Is there a Chinese Sense of Privacy?" (2001) 26 IIAS Newsletter Online www.iias.nl (accessed 7 August 2007).

26 El Guindi, above n 25, 82-96; Jingchun, above n 25; Office of the Victorian Privacy Commissioner *Privacy in Diverse Victoria*, above n 23, 20; Patrick Reilly and Rowena Cullen *Information Privacy and Trust in Government: A Citizen-Based Perspective* (report presented to the State Services Commission, 2006) 27, 46, 48.

27 *Hosking v Runting* [2005] 1 NZLR 1, 32 (CA).

5.19 In the absence of further research, we are unable to say how attitudes to and concepts of privacy may differ between the various cultures represented in New Zealand, but it is reasonable to assume that there are significant differences and that research on this topic would be helpful to future discussions on privacy law reform.

MĀORI AND PRIVACY

5.20 As an illustration of cultural influences on concepts of privacy, and because of their unique position as New Zealand's indigenous people, we give particular consideration to Māori understandings of privacy.[28] Again, there has been little specific research on this topic. Our discussion here is based on a survey of existing literature, including literature that is not specifically focused on privacy. Further research is required, and the Commission would welcome submissions from Māori (as well from other cultural groups) in the later stages of this Review. In this part of the chapter we consider possible influences on Māori concepts of privacy, and some ways in which those concepts might be distinctive. Later in the chapter we will look at opinion survey evidence about Māori attitudes to privacy.

5.21 A variety of words are used as translations of "privacy" and "private" in modern Māori, but it is perhaps less fruitful to start with the English word and look for Māori equivalents than to consider how certain Māori customary concepts or values may relate to privacy. The Law Commission has observed elsewhere that equivalences between human rights principles and the customary concepts of Māori and other Pacific peoples can be identified by looking at underlying values.[29] The Commission noted in particular that respect for the dignity of all persons is central to both human rights and Pacific custom. In Māori and other Polynesian languages this is often expressed as respect for the mana (personal power or standing) of each individual.[30] While levels of mana differ between individuals, all people possess a mana which should be respected by others.[31] This concept is compatible with the equal entitlement of humans to respect, which we identified in chapter 3 as one of the core values of which privacy is a sub-category.

5.22 Other Māori customary concepts are also relevant to privacy. The complementary concepts of tapu and noa were fundamental, structuring principles of traditional Māori society, much as public and private are in contemporary Western societies. However the public/private distinction cannot be overlaid in any simple way on the concepts of tapu and noa. Tapu can be defined as "set apart under ritual restriction", while noa is a state of being free from such restriction.[32] The quality of being set apart, with access to a person or place being restricted, has some affinities with privacy. Among other things, tapu functioned to preserve social distance and respect.[33]

28 For a study of attitudes to privacy in another indigenous group see Roy Morgan Research *"It's Like Delving into Your Soul": Aboriginal and Torres Strait Islander Privacy Awareness Consultation and Research – Final Report* (prepared for the Human Rights and Equal Opportunity Commission, Roy Morgan Research, Canberra, 1995).

29 New Zealand Law Commission *Converging Currents: Custom and Human Rights in the Pacific* (NZLC SP17, Wellington, 2006).

30 Ibid, 50-51, 75-76.

31 Hirini Moko Mead *Tikanga Māori: Living by Māori Values* (Huia, Wellington, 2003) 29-30, 51-52. See also Te Ahukaramū Charles Royal "A Modern View of Mana" (paper presented to joint conference of the Australian Psychological Society and the New Zealand Psychological Society, Auckland, 26-30 September 2006).

32 Joan Metge *New Growth from Old: The Whānau in the Modern World* (Victoria University Press, Wellington, 1995) 85.

33 Ibid, 86.

Hirini Moko Mead describes the personal tapu of each individual as being like "a personal force field which can be felt and sensed by others", and notes that violation of this space can cause discomfort, affront and damage.[34] While there are similarities between tapu and privacy, however, it is noa that conveys the sense of relaxation and freedom of action commonly associated with being in private.[35] Both tapu and noa, then, may have functioned to protect aspects of privacy traditionally, and may continue to have some influence on how Māori think about privacy today.

5.23 Another relevant concept is whakamā, a term that is not easily translated. It is associated with feelings of inadequacy and hurt, and with behaviour marked by withdrawal from communication with others.[36] A person could well feel whakamā as a result of the exposure of some private fact which causes him or her shame. At the same time, whakamā could function as a way of gaining some privacy in close-knit communities, providing "a culturally acceptable escape hatch, a refuge and defence against intrusion".[37]

5.24 It is apparent from these examples that the relationship between Māori customary concepts and the concept of privacy is not a straightforward one. Nor is it easy to assess what influence such concepts have on Māori attitudes to privacy today. Such concepts and values may be useful, however, in making privacy law more relevant to tikanga Māori.

5.25 It is also likely that there are some distinct Māori perspectives on what constitutes a private place and private information. For example, is a marae a private or a public place? Anne Salmond observes that the marae is "a Māori public place" but that at the same time its privacy is usually protected by its remote location or by high fences.[38] Much of what could be considered Māori "public" business takes place on the marae, but this does not necessarily mean that it is a public place for people who do not belong to that particular marae.[39] It is possible that the question of whether a marae is a private place, and whether there is a reasonable expectation of privacy in relation to events taking place on a marae, could come before the courts in future.[40] The answer may well depend on the purpose for which the marae was being used at the relevant time.

---

34 Mead, above n 31, 46, 48.

35 Metge *New Growth from Old*, above n 32, 85; New Zealand Law Commission *Māori Custom and Values in New Zealand Law* (NZLC SP9, Wellington, 2001) 36.

36 Joan Metge *In and Out of Touch: Whakamaa in Cross Cultural Context* (Victoria University Press, Wellington, 1986) 25-37.

37 Ibid, 116.

38 Anne Salmond *Hui: A Study of Māori Ceremonial Gatherings* (2 ed, Reed Books, Birkenhead, 1976) 33-34.

39 In the view of a tikanga expert consulted by the Broadcasting Standards Authority, the marae is not a public place and what goes on there is not in the public domain: Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press/Broadcasting Standards Authority, Wellington, 2004) 58.

40 In *R v Tame Iti* (4 April 2007) CA 267/06, paras 24-39 Hammond J for the Court, the Court of Appeal considered the question of whether the marae ātea (the ceremonial courtyard in front of the meeting house) is a public place for the purposes of the Arms Act 1983. The Court rejected the appellant's argument that the marae ātea was a separate, private area, and that his actions therefore were not carried out in a public place. In the Court's view, the marae as a whole was a public place for the purposes of the Act at the material time. This decision is unlikely to be relevant to the very different question of whether there is a reasonable expectation of privacy in relation to events that take place on a marae, particularly where it is alleged that privacy has been invaded by persons who have not been invited onto the marae.

5.26 The questions of what information Māori see as private, and to whom that information belongs, are even more complex. The Privacy Act 1993 (section 2) defines "personal information" as "information about an identifiable individual" and "individual" as "a natural person, other than a deceased person".[41] The Privacy Act does not, therefore, protect against disclosure of information about groups or deceased persons, or disclosure of non-identifiable information. It has been argued that the individualistic focus of privacy law does not take account of the collective interests of Māori groups.

5.27 A Māori government official consulted by the Broadcasting Standards Authority commented that "The impact upon a breach of privacy for a Māori isn't only ever about that individual, it is always about their familial ties and their community connection or their local geography."[42] Some Māori also consider that "a deceased person's place in Māori genealogy meant their privacy might be breached and, by extension, the privacy of his [or] her whānau, hapū and iwi".[43]

5.28 In addition, it may be considered that some types of personal information belong not to the individual but to the group.[44] Perhaps the clearest example is whakapapa (genealogical) information. Whakapapa information and books in which whakapapa is recorded are often considered tapu. Access to this information is carefully guarded, and custodians of whakapapa hold it on behalf of their whānau, hapū or iwi.[45] From a Māori perspective it could be considered private information, even though it relates to deceased persons and to a group rather than an individual.

5.29 The placing of whakapapa information on the internet is a controversial issue. There was significant Māori opposition to proposals to make Māori Land Court records available online because of concern about public access to records containing whakapapa information.[46] On the other hand, rights in Māori land depend in large part on the whakapapa evidence contained in Māori Land Court records, and people are entitled to know the basis for their inclusion in or exclusion from such rights. It can be argued, therefore, that placing these records online simply facilitates the exercise of this existing right.

5.30 There is also a range of perspectives on making whakapapa information available online through genealogy sites or other specialist websites.[47] Online availability

41 "Individual" is defined in the Broadcasting Act 1989, s 2(1), as having the same meaning as in section 2(1) of the Privacy Act 1993, so the Broadcasting Standards Authority's privacy jurisdiction also relates only to living, natural persons.

42 Broadcasting Standards Authority *Real Media, Real People*, above n 39, 57.

43 Ibid.

44 See also discussion of a possible right to privacy for indigenous or other ethnic groups in Australian Law Reform Commission *Review of Australian Privacy Law* (ALRC DP 72, Sydney, 2007) 124-125, 129-130, 132-135.

45 Salmond, above n 38, 122; Metge *New Growth from Old*, above n 32, 90-91; Majit Singh Gill *Working Toward Usability for Computer-Based Māori Whakapapa Systems* (Master of Business thesis, Auckland University of Technology, 2006) 76; Paua Interface Ltd *Research of Issues for Māori Relating to the Online Authentication Project* (report for the State Services Commission, 2004) 24-25. The importance of whakapapa in Māori culture also affects Māori attitudes to advances in genetic science (discussed in chapter 6): see Maui L Hudson, Annabel L M Ahuriri-Driscoll, Marino G Lea and Rod A Lea "Whakapapa: A Foundation for Genetic Resarch?" (2007) 4 Bioethical Inquiry 43.

46 Paua Interface Ltd, above n 45, 24-25; "Māori Land On Line Feedback Closes" (June 2004) *Te Pouwhenua* 6.

47 See for example contributions to the discussion "Should Whakapapa be Online?" at www.maori.org.nz (accessed 5 November 2007).

of whakapapa information can be seen as violating tapu, breaching protocols surrounding oral transmission of knowledge, and placing information at risk of misuse by people seeking to claim rights based on fabricated whakapapa connections. However, the internet can also be seen as a useful tool which allows individuals living away from their tribal homelands to learn about their history and ancestry, and to reconnect with their whānau, hapū and iwi. Sharing whakapapa and related information online can be seen as a way of preserving this knowledge for current and future generations.

5.31 It has also been suggested that aggregated data about Māori groups should be protected within a privacy framework. In this view, there can still be a collective privacy interest even when no information about identifiable individuals is presented. A report to the State Services Commission commented that:[48]

> The Privacy Act (1993) is individually focused. Informants ask what the protective mechanisms for collective privacy are. The issue of "collective ownership" and "collective privacy" incorporates the idea of a whānau or hapū "owning" their collective information also referred to as aggregated or statistical data. This enables their rights to make decisions about that information including how it is shared, how it is aggregated and how it is published.

Such arguments tend to use the concepts of privacy and ownership interchangeably, and the claim to collective control of aggregated data is clearly related to broader notions of collective Māori property rights in information. Māori intellectual property rights are currently being considered by the Waitangi Tribunal in the Wai 262 (indigenous flora and fauna and cultural intellectual property) inquiry, and there is ongoing work on indigenous intellectual property rights in the World Intellectual Property Organisation, to which New Zealand is contributing.[49]

5.32 So far our discussion has focused on possible cultural influences on Māori attitudes to privacy, but it is important to consider also the likely influence of the Māori experience of being an indigenous minority who have at times suffered discrimination and unfair treatment, including from the government.[50] Historically, Māori have often been reluctant to provide information to the government due to concerns about loss of autonomy, and some of this feeling may still persist.[51] Another possible influence on Māori attitudes to privacy is social class. On average, Māori socioeconomic status is lower than that of Pākehā, and as a result Māori may feel more vulnerable to having their personal

48 Paua Interface Ltd, above n 45, 23; see also Susan Shingleton "Māori Concerns Regarding Retention of and Access to Health Information" (Summer 1995) *New Zealand Archivist* 8.

49 See "Flora and Fauna (Wai 262)" at www.waitangi-tribunal.govt.nz and "Traditional Knowledge" at www.med.govt.nz (accessed 5 November 2007); Te Ahukaramū Charles Royal *Traditional Knowledge: Some Comment* (report prepared for Te Puni Kōkri/ Ministry of Māori Development, February 2007).

50 For attitudes to privacy among a non-indigenous minority see Oscar H Gandy "African Americans and Privacy: Understanding the Black Perspective in the Emerging Policy Debate" (1993) 24 Journal of Black Studies 178.

51 A participant in a Law Commission forum in May 2007 made this point, and gave as examples opposition to registering births among some Māori as late as the 1950s; opposition by the Rātana and Ringatū churches to registering their ministers; and reluctance to send Māori children to school in some areas because of concern that school registrations could be used later for the call-up for military service. It was suggested that similar attitudes could be found today among some Māori who are reluctant to register on the electoral roll.

information used by state agencies and others in ways that may adversely affect them. Māori may also feel that they come under greater scrutiny and surveillance than the majority of the population; as one Māori interviewee remarked in a State Services Commission study, "We are used to being watched!"[52]

YOUNG PEOPLE, NEW TECHNOLOGIES AND PRIVACY

5.33 Another factor that is likely to influence attitudes to privacy is age. People have different experiences and expectations of privacy at different ages. Young children generally have very little privacy and are under parental surveillance most or all of the time. As children get older they are usually accorded progressively more privacy. At the other end of life, old people may lose much of their privacy if they become sick or infirm, and particularly if they move into residential care.

5.34 In addition, different generations may have different attitudes to and concepts of privacy because they have grown up in different worlds. It is this aspect that we focus on here. In particular, we consider whether distinct attitudes to privacy may be emerging among young people (a term we are using loosely here to cover everyone from children to people in their early twenties).[53] Today's young people are growing up, or have grown up, in a networked world: the world of the internet and mobile phones. Many people are suggesting that this is producing a very different sense of privacy from that of older generations. We will examine the implications of new technologies for privacy in the next chapter, but for now we will consider the role of technology in shaping young people's attitudes. In doing so, we will rely mainly on research and commentary from overseas. At present there is relatively little research on these issues in New Zealand, although projects such as NetSafe's "Convergence Generation" research should add considerably to our understanding.[54] We will refer later in this chapter to what opinion poll data from New Zealand shows about the attitudes to privacy of younger people.

5.35 Young people have grown up in a world in which the internet and mobile phones (particularly text messaging) allow them to keep in touch with their friends constantly. They use these technologies to form, develop and maintain friendships, and enjoy being able to communicate all the time.[55] This experience of constant connectivity probably means that their ideas about limiting access to themselves and their information are different from those of older generations.

52 Rowena Cullen and Peter Hernon *Wired for Well-Being: Citizens' Response to E-Government* (report presented to the State Services Commission, 2004) 52.

53 See also discussion of young people's attitudes to privacy in Australian Law Reform Commission *Review of Australian Privacy Law*, above n 44, ch 59.

54 "NetSafe's 'Convergence Generation' Research Underway" (April 2007) *NetSafe Newsletter* www.netsafe.org.nz. See also the work of the Youth Connectedness Project, Roy MacKenzie Centre for the Study of Families, Victoria University of Wellington, www.vuw.ac.nz/youthconnectedness. For a summary of some of the projects currently examining New Zealand young people's online behaviour, see Jo Kleeb "Youth and the Internet: The Positives, the Challenges and New Zealand Developments" (presentation to Ministry of Youth Development seminar series, 12 November 2007), available on the Youth Connectedness Project website.

55 Pew Research Center for the People and the Press *How Young People View their Lives, Futures and Politics: A Portrait of "Generation Next"* (Pew Research Center, Washington, DC, 2007) 13-15; C4 Music Television "NZ Youth Take Part in MTV's Circuits of Cool" (24 July 2007) Press Release at www.scoop.co.nz (accessed 25 July 2007).

5.36 Much of the discussion about young people and privacy focuses on the information they make available on blogs and online social networks.[56] *Blogs* (an abbreviation of "weblogs") are websites that are updated from time to time by their creators, with entries appearing in chronological order. They are thus rather like online journals. While much of the media coverage of blogs concentrates on those which comment on public events or particular areas of interest, the majority of blogs are about the bloggers' everyday lives, thoughts and emotions. This is particularly true of blogs written by women and teenagers.[57] *Online social networks* such as MySpace, Bebo and Facebook are:[58]

> spaces on the internet where users can create a profile and connect that profile to others to create a personal network. Social network users post content to their profiles and use tools embedded within social networking websites to contact other users. Young adults and teenagers are among the most avid users of such websites.

Neither blogging nor online social networking are limited to young people, and many bloggers in particular are aged over 25. However, it is younger people whose sense of self and of privacy may be shaped by growing up in a world in which online identities are an integral part of social interaction.

5.37 The fact that such sites are based on self-disclosure has led many commentators to ponder their implications for young people's attitudes to privacy.[59] Just like face-to-face relationships, building online relationships involves revealing (or inventing) things about yourself. According to one researcher:[60]

> In many ways blogging is a performance, a performance in the sense that you're expecting people to read it and you're expecting interaction. It's not just personal self-disclosure, it's the desire to build an audience, a community, and those communities are one of the beautiful things that can come out of blogging.

---

56 Young people also make use of online chat rooms and forums, which can raise similar privacy and safety concerns.

57 Fernanda B Viégas "Bloggers' Expectations of Privacy and Accountability: An Initial Survey" (2005) 10 Journal of Computer-Mediated Communication http://jcmc.indiana.edu (accessed 19 July 2007); Solove *The Future of Reputation*, above n 19, 24. A recent survey of 1529 New Zealanders found that 10 per cent had their own blog, and that 21 per cent of bloggers were under 20 years of age: Allan Bell, Charles Crothers, Andy Gibson, Ian Goodwin, Karishma Kripalani, Kevin Sherman and Phillipa Smith *New Zealanders and the Internet: A Preliminary Profile of Usage and Attitudes* (2007 Benchmark Survey: Interim Report, World Internet Project New Zealand, Institute of Culture, Discourse and Communication, AUT University, Auckland, December 2007) 16.

58 Pew Internet & American Life Project *Teens, Privacy & Online Social Networks: How Teens Manage their Online Identities in the Age of MySpace* (Pew Internet & American Life Project, Washington, DC, 2007) i. MySpace reported in February 2007 that it had 500,000 New Zealand members, and Bebo is believed to have even more members in New Zealand. Facebook reported 33,000 members in New Zealand in July 2007, but was growing rapidly. Alice Hudson "Online Traps for Unwary Teens" (12 August 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 12 August 2007).

59 See for example Tapu Misa "Brash Cyber-Fallout Potent Reminder of Waning Privacy" (29 November 2006) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 10 August 2007); Alan Perrott "A Very Public Affair" (24 Feburary 2007) *Canvas (New Zealand Herald magazine)* Auckland 12-15; Emily Nussbaum "Say Everything" (12 February 2007) *New York* http://nymag.com (accessed 13 February 2007); "We're All Celebrities in the Post-Privacy Age" (22 June 2007) www.stuff.co.nz (accessed 22 June 2007); Janet Kornblum "Online Privacy? For Young People, That's Old School" (22 October 2007) *USA Today* www.usatoday.com (accessed 24 October 2007); Susan B Barnes "A Privacy Paradox: Social Networking in the United States" (4 September 2006) *First Monday* www.firstmonday.org (accessed 15 June 2007).

60 Meredith Bean, a doctoral student at Auckland University who has studied blogging, quoted in Perrott, above n 59, 14.

Likewise, social networking allows young people "to present themselves to a group of peers and then get feedback and affirmation", "to feel like they are a part of a group of like-minded friends" and to "visualize their network of relationships, displaying their popularity for others".[61]

5.38 There is nothing new about attracting attention or building relationships through self-disclosure. However, parents and other adults express disquiet about the nature of the information and images being put online, the potential for this content to be viewed by people other than the intended audience, and the fact that online information is archived and can be retrieved years later. As newspaper columnist Tapu Misa comments:[62]

> [J]ust because kids are technologically fluent doesn't mean they understand the privacy implications of their digital activities. What, years from now, will come back to bite my son in the bum? At 12, he hasn't thought that far ahead.

5.39 Young people's online activities have led to claims of a generation gap, as "the older generation looks on with alarm and misapprehension not seen since the early days of rock and roll."[63] Young people are portrayed as being recklessly honest or uninhibited online (honesty and lack of inhibition are not necessarily the same thing, since the information they post or the personae they adopt will sometimes be false). Some say that this is because young people think of the material they post online as being private and confidential, and fail to think about strangers (or parents) gaining access to this material.[64] Others claim that "The young generation are happy to share their lives publicly."[65]

5.40 Is it the case that "Old-fashioned notions such as privacy are under siege as social rules are outpaced by technological change"?[66] Or is technological change giving rise to new social rules and new understandings of privacy? One suggestion is that in an online world ideas about privacy will be based on individuals exercising control over access to their information.[67] If this is the case, it is important to explore how young people are in fact exercising that control.

5.41 A major United States study of online privacy among 12-17 year-olds found that 93 per cent use the internet, while 55 per cent of those who are online use social networks and the same number have posted a profile online.[68] Older teens are

61 Pew Internet & American Life Project *Teens, Privacy & Online Social Networks*, above n 58, 13-14.

62 Misa, above n 59.

63 Nussbaum, above n 59.

64 Vito Pilieci "Young People Clued Out Over Internet Privacy" (5 February 2007) www.canada.com (accessed 8 February 2007); Barnes, above n 59.

65 Jyri Engstrom of the Jaiku "microblogging" service, quoted in Darren Waters "Hyper-Connected Generation Rises" (9 May 2007) http://news.bbc.co.uk (accessed 14 June 2007); see also Nussbaum, above n 59.

66 Alan Perrott, above n 59, 13.

67 "We're All Celebrities in the Post-Privacy Age", above n 59; Eric Auchard "It's No Secret: Facebook's Allure is its Privacy" (16 July 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 16 July 2007).

68 Pew Internet & American Life Project *Teens, Privacy & Online Social Networks*, above n 58. Where not indicted otherwise, figures in this section are from this study.

more likely to use these networks (61 per cent of teens aged 14-17 compared to 41 per cent of 12-13 year-olds). Of those who had online profiles:

- 79 per cent had posted photos of themselves and 66 per cent had posted photos of friends.
- 82 per cent had posted their first name, and 26 per cent had posted both their first and last names. Most of those posting their full names restricted access to their profile, with only 11 per cent posting their full name to a profile that is visible to anyone online.
- 56 per cent had posted at least some false information, and 8 per cent said that most or all of the information in their profile was false. Boys were more likely than girls to say that they had posted false information (64 per cent of boys and 50 per cent of girls).
- 66 per cent restricted access to their profiles in some way.
- 31 per cent had "friends" on their profile whom they had never met in person (although in many cases these unmet "friends" had at least some connection to their offline friends – for example, they were friends or relatives of friends).
- 44 per cent had been contacted by a stranger online.

5.42 Overall, this study does not present a picture of a generation with no concern for privacy. A small minority of teens do appear to be giving little thought to the possible consequences of, for example, posting their full names on an unprotected profile. The majority, however, are exercising some caution.

5.43 While much parental concern about online social networking focuses on "stranger danger", particularly from paedophiles, most teenagers in the United States study appeared to be aware of the need to protect themselves against contact by strangers. Of those who had been contacted by a stranger online, most (65 per cent) ignored or deleted the message, while 21 per cent responded to find out more about the person. Twenty-three per cent of those who had been contacted by strangers felt scared or uncomfortable as a result. Girls in particular were concerned about their physical safety and were generally reluctant to provide information online that could allow them to be contacted in person.

5.44 Social networking for teenagers is primarily about keeping in touch with friends whom they already know in their offline life.[69] However, the prevalence of online friendships with strangers increases with age. One New Zealand study found that 48 per cent of 14-15 year-olds who use the internet had friends they had not met in person, compared to 27 per cent of those aged 10-11. On the other hand, younger children appeared to distinguish less clearly between online and offline friends, suggesting that they may be more vulnerable to the risks of interacting with strangers online.[70]

69 According to a major international study that included New Zealand young people, 65 per cent of New Zealand children aged 8-14 interact only with people they know on social networking sites, and 80 per cent would not respond if contacted by a stranger: C4 Music Television "NZ Youth Take Part in MTV's Circuits of Cool", above n 55.

70 Jo Kleeb "Presentation to Stakeholders: School, Bullying, Technology" (July 2007), slides 21-23, at www.vuw.ac.nz/youthconnectedness (accessed 5 November 2007).

5.45 However, while most young people may be exercising caution in some aspects of their online activities, there is still cause for concern. There was little evidence from the United States study that teenagers were giving much attention to possible consequences that did not involve strangers locating them in person. A survey of young people in the United Kingdom found that 71 per cent had never been concerned about strangers viewing their personal online profiles.[71] The willingness, particularly among girls, to post photos online is an example of this. In focus groups, teenagers in the United States study explained that the photos they posted did not contain enough information, even when combined with other information in their profiles, to compromise their privacy or safety. However, this does not address the concern about photos being viewed by people for whom they were not intended, either now or in the future, with consequent potential for embarrassment or worse. Only 39 per cent of teens who posted photos online said that they restricted access to the photos most of the time, with another 38 per cent restricting access sometimes. Even when access to photos is restricted, "friends" may be able to copy them and pass them on.[72]

5.46 In addition, it is not only the young person who has created a particular blog or social networking profile whose privacy may be affected. Inevitably, such sites contain information about and photos of other people, particularly friends and family. In most cases it is unlikely that the permission of these other people has been sought, even though in some cases they will be identified by name.[73] Older bloggers tend to at least give consideration to the privacy issues involved in writing about other people,[74] but younger people posting material online may be less likely to think about the possible impact on others.

5.47 One potential check on teenagers' online activity is the knowledge that parents or other known adults may read their profiles. While many adults have been relatively unfamiliar with social networking sites until recently, it appears that their knowledge of, and concern about, these sites is growing. In the United States study referred to above, which also included the parents or guardians of the teenagers surveyed, 73 per cent of parents of teenagers with online profiles correctly stated that their child had a profile online.[75] As parents become more familiar with online social networking, they are increasingly seeking to gain access to their children's online profiles.[76] This also raises privacy issues, however, since for many young people their sense of privacy is primarily focused

71 Tri Media Harrison Cowley *Data Protection Topline Report* (prepared for the Information Commissioner's Office, United Kingdom, October 2007) 7.

72 Ed Pilkington "Blackmail Claim Stirs Fears Over Facebook" (16 July 2007) *Guardian* United Kingdom www.guardian.co.uk (accessed 16 July 2007).

73 In one survey of bloggers, 66 per cent said that they almost never asked permission when writing about other people, and 21 per cent said they almost always revealed names: Viégas, above n 57.

74 Meredith Reneé Bean *Personal Journaling Online or "Blogging" and its Perceived Effects on Relationships and Self* (MA Thesis, University of Auckland, 2006) 75-77, 82-84, 95-96, 99-100; Viégas, above n 57.

75 However, a United Kingdom survey found significant gaps in understanding of technology between parents and children, and discrepancies between what parents thought their children were doing on the internet and mobile phones and what children said they were doing: NCH *Get I.T. Safe: Children, Parents and Technology Survey 2006*.

76 Hudson, above n 58; Daniel Sieberg "Invasion of Privacy or Smart Parenting?" (19 November 2007) www.cbsnews.com (accessed 21 November 2007).

on keeping information private from parents and other adult authority figures.[77] It could be argued that parents reading their children's online profiles and journals is similar to reading their diaries or listening in to their phone calls, and such ethical considerations have to be balanced against legitimate concerns with young people's safety and welfare.[78]

5.48 It is very difficult at this stage to know whether apparent differences in privacy-related attitudes and behaviour between younger and older generations herald a long-term shift in views of privacy. Some of these differences may be due to the age-old tendency of young people to take risks and not to consider future consequences. As American writer Emily Nussbaum asks:[79]

> What happens when a person who has archived her teens grows up? Will she regret her earlier decisions, or will she love the sturdy bridge she's built to her younger self – not to mention the access to the past lives of friends, enemies, romantic partners?... Is there a point in the aging process when a person will want to pull back that curtain – or will the MySpace crowd maintain these flexible, cheerfully thick-skinned personae all the way into the nursing home?

Only time and long-term research can answer these questions, but privacy law and public policy will need to be aware of changing attitudes to privacy among young people if it is to remain relevant to contemporary New Zealand.

PUBLIC OPINION SURVEYS AND PRIVACY

5.49 Before we analyse the available evidence about public attitudes to privacy in New Zealand, it is important to consider some of the difficulties and pitfalls involved in using such data. Internationally, there is now a significant body of research on public attitudes to privacy.[80] This literature is useful to New Zealand both for comparative purposes and for the lessons it provides about the usefulness or otherwise of opinion surveying for privacy policy-making.

5.50 The international literature identifies a number of potential problems with surveys of privacy attitudes:

- Often surveys ask people for their views on privacy (for example, how important privacy is to them) without either asking them what they understand by privacy,[81] or providing them with a definition of privacy for

77 Misa, above n 59; Barnes, above n 59.

78 Ann Weatherall and Annabel Ramsay *New Communication Technologies and Family Life* (Families Commission, Wellington, 2006) 17-18.

79 Nussbaum, above n 59.

80 Electronic Privacy Information Center "Public Opinion on Privacy" www.epic.org/privacy/survey (accessed 13 August 2007); Roger Clarke "Reference List: Surveys of Privacy Attitudes" www.anu.edu.au/people/Roger.Clarke/DV/Surveys.html (accessed 13 August 2007); Perri 6 with Kristen Lasky and Adrian Fletcher *The Future of Privacy* (vol 2, Demos, London, 1998); Oscar H Gandy, Jr "Public Opinion Surveys and the Formation of Privacy Policy" (2003) 59 Journal of Social Issues 283; Kevin D Haggerty and Amber Gazso "The Public Politics of Opinion Research on Surveillance and Privacy" (2005) 3 Surveillance and Society 173; Elia Zureik, Lynda Harling Stalker and Emily Smith "Background Paper for the Globalization of Personal Data Project International Survey on Privacy and Surveillance" (Surveillance Project, Queen's University, Kingston, Ontario, Canada, 2006) www.queensu.ca/sociology/Surveillance (accessed 13 August 2007); Bennett and Raab, above n 4, 62-79; National Research Council of the National Academies *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washington, DC, 2007) 162-166.

81 A rare example of a survey that asked people what they understood by privacy was the survey carried out for the report of the Younger Committee in the UK in 1972: "Appendix E: Report of the Survey of Public Attitudes to Privacy" in Report of the Committee on Privacy (1972) Cmnd 5012, 228, 229-230, 234-235.

the purposes of the survey. As we have seen in chapter 2, there are many theories about how privacy is best defined. We have also seen in this chapter that there appear to be different understandings of privacy based on factors such as culture and age. When answering very general questions about "privacy", therefore, it is likely that different people will have very different concepts in mind.

- People's expressed attitudes or concerns may not match their behaviour. Some researchers have described a "privacy paradox", whereby:[82]

  > On the one hand, privacy seems to be so highly regarded by individuals that many claim to only reluctantly trade off convenience or other benefits for it…. [But on] the other hand, consumers have also been found to be willing to provide personal information for small discounts and rewards.

  The evidence about the extent to which consumers are willing to trade privacy for convenience or price is mixed,[83] and research in this area is continuing, but it is important to at least consider the likelihood that professed attitudes and behaviours will diverge.

- As with all surveys, responses are likely to be influenced by the ways in which the questions are framed. In the case of privacy surveys, it is worth keeping in mind that they are often conducted on behalf of organisations with a particular stake in the outcomes, whether it be companies wishing to gain greater access to personal information or privacy-protection agencies wanting to establish that their role is justified by public concern.
- Survey responses may also be influenced by current events and by recent media "horror stories" about either invasions of privacy or incidents in which privacy is seen to stand in the way of other public goods.
- A particular problem for surveys of attitudes to privacy is that people who are very concerned about privacy are likely to be over-represented among those who refuse to take part in surveys, since survey questions can themselves be seen as intruding on privacy.[84]
- Privacy issues are often complex, especially when they involve new technologies, and many people have little understanding of how their personal information is used. It may, therefore, be difficult to get useful responses on key issues from random phone surveys.
- Some surveys present an account of opinion among a homogeneous "public", and fail to explore the differences in attitudes that may be found if the survey responses are broken down by sex, age, ethnicity, income, occupation or place of residence, for example.

---

82 Jens Grossklags and Alessandro Acquisti "When 25 Cents is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information" (Paper presented to the Workshop on the Economics of Information Security, Carnegie Mellon University, 7-8 June 2007).

83 See for example E Rose "Data Users Versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?" in *Proceedings of the 38th Hawaii International Conference on System Sciences* (2005); Bettina Berendt, Oliver Günther and Sarah Spiekermann "Privacy in E-Commerce: Stated Preferences vs Actual Behavior" (2005) 48 Communications of the ACM 101; Grossklags and Acquisti, above n 82; Janice Tsai, Serge Engelman, Lorrie Cranor and Alessandro Acquisti "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study" (Paper presented to the Workshop on the Economics of Information Security, Carnegie Mellon University, 7-8 June 2007).

84 Haggerty and Gazso, above n 80 give particular attention to this problem.

5.51 These potential problems are not insurmountable, however, and survey data can still play a useful role in informing policy debates. Questions about particular scenarios can help to give more substance to general questions about attitudes to "privacy". Qualitative focus group work can also usefully supplement phone polls and other quantitative data.[85] Focus groups can be used to tease out what people mean by privacy, and can be given background information so that their discussion of issues is better informed.[86] Further research on the relationship between attitudes and behaviour is also useful.

PUBLIC OPINION IN NEW ZEALAND

5.52 The most thorough surveys of attitudes to privacy in New Zealand have been carried out on behalf of two regulatory bodies, the Office of the Privacy Commissioner (OPC) and the Broadcasting Standards Authority (BSA). Other government agencies, particularly the State Services Commission and Statistics New Zealand, have also conducted research in this area. In this chapter we will restrict our analysis to the results of these state-sector-sponsored surveys (especially those of the OPC and BSA), while recognising that research is also conducted by New Zealand academics and private companies.[87]

5.53 The most recent OPC-sponsored opinion survey, conducted in 2006, found that 56 per cent of people said that they were concerned about individual privacy, up from 47 per cent in 2001, and only 19 per cent said that they were not concerned (down from 25 per cent in 2001).[88] The increase in the expressed level of concern about privacy is interesting, although it is somewhat difficult to interpret as the question asked was a very general one in which "individual privacy" was not defined.[89] Seventy-two per cent of people said that there was a need for the Privacy Commission, while 22 per cent said the Commission was not needed. When presented with scenarios relating to the handling of information by businesses, between 85 and 90 per cent of people were concerned about businesses:

- using personal information for purposes other than those for which it was supplied;
- obtaining personal information without authorisation;
- asking for personal information that seems irrelevant to a particular transaction; and
- tracking the internet sites people visit without their knowledge.

85 See for example Perri 6 with Lasky and Fletcher, above n 80, ch 2.

86 For example, in focus group research conducted for the State Services Commission, group members were first asked to describe what "privacy" means to them, and were then given a definition of information privacy for the purposes of the remainder of the discussion: Reilly and Cullen, above n 26, 27.

87 Ellen Rose of Massey University has conducted research on attitudes to privacy: Rose "Data Users Versus Data Subjects", above n 83; Ellen A Rose "An Examination of the Concern for Information Privacy in the New Zealand Regulatory Context" (2006) 43 Information & Management 322. The Unisys Security Index New Zealand, published several times per year, includes questions about New Zealanders' concerns in relation to online security and unauthorised access to personal information: www.unisys.com.au (accessed 13 August 2007).

88 All information about the OPC survey is from Privacy Commissioner/UMR Research *A Summary Report* (2006), available at www.privacy.org.nz. This document reports on a national telephone survey of 750 New Zealanders aged 18 and over, conducted in February 2006. Eleven per cent of those surveyed were Māori. Questions used a five-point scale from "very concerned" (1) to "not concerned at all" (5). Except where indicated otherwise, we combine responses of 1 and 2 (very concerned and somewhat concerned) for a total "concerned" figure, and responses of 4 and 5 (somewhat unconcerned and not concerned at all) for a total "not concerned" figure.

89 Respondents were asked "How concerned are you about the following?", and then asked about a series of issues, including "Individual privacy".

5.54 Perhaps the most useful question in the OPC survey was one which asked people how concerned they were about a series of specific privacy issues. This question provides responses to something more concrete than "privacy", and also gives an indication of the *relative* levels of concern about different issues. The responses to this question have not changed greatly since the 2001 survey. As in 2001, the security of personal information on the internet emerged as the privacy issue about which the largest percentage of people were concerned.[90]

TABLE 1: RESPONSES TO OPINION SURVEY QUESTION "HOW CONCERNED ARE YOU ABOUT THE FOLLOWING PRIVACY ISSUES IN NEW ZEALAND TODAY?" (PERCENTAGES). N=750

	Concerned	Neutral	Not concerned	Unsure
The security of personal details on the Internet	84	8	6	2
Confidentiality of medical records	78	12	10	–
Government interception of telephone calls or email	72	15	13	–
The privacy of personal details held for credit reporting	67	19	13	1
Tracking people on the Internet	62	19	16	3
The availability of personal details on public registers (for example, the Motor Vehicle Register and the Electoral Roll)	54	22	23	1
Employer monitoring of emails	50	23	25	2
A compulsory ID number for every New Zealander	50	18	31	1
Data sharing between Government departments	37	29	32	2
Random drug testing of employees	36	19	44	1
Video surveillance in public places	30	24	45	1

5.55 When the survey results are broken down into different segments of the population, only small differences were apparent in response to the general question about level of concern about individual privacy, but more significant differences can be seen in responses to more specific questions. Women, younger people and Māori were more likely to say that there was a need for the Privacy Commission.[91] On the questions regarding level of concern about particular privacy issues, there was a small but consistent tendency for women to be more concerned than men, and some significant differences in the level of concern between Māori and non-Māori, as the following table shows.

90 A significant level of concern about the security of personal information on the internet was also expressed in surveys and focus group research for Statistics New Zealand and the State Services Commission: Statistics New Zealand/UMR Research *Public Attitudes to the Confidentiality, Privacy and Security of Official Government Survey Data* (2005) 13, 17, 44-56; Reilly and Cullen, above n 26, 32, 35-37.

91 Male 66 per cent, female 77 per cent; under 30 85 per cent, 30-59 76 per cent, 60 + 51 per cent; Māori 84 per cent, non-Māori 70 per cent.

TABLE 2: RESPONSES TO OPINION SURVEY QUESTION "HOW CONCERNED ARE YOU ABOUT THE FOLLOWING PRIVACY ISSUES IN NEW ZEALAND TODAY?" – PERCENTAGES OF RESPONDENTS "CONCERNED" BY SEX AND ETHNICITY. N=750

	Female	Male	Māori	Non-Māori
The security of personal details on the Internet	87	78	86	83
Confidentiality of medical records	79	76	82	77
Government interception of telephone calls or email	73	69	77	71
The privacy of personal details held for credit reporting	69	64	64	67
Tracking people on the Internet	65	60	71	61
The availability of personal details on public registers	57	50	56	54
Employer monitoring of emails	53	49	53	50
A compulsory ID number for every New Zealander	51	48	61	48
Data sharing between Government departments	40	33	46	36
Random drug testing of employees	37	34	54	33
Video surveillance in public places	32	29	39	29

These figures suggest significantly higher levels of concern among Māori about certain types of monitoring and surveillance by government and other agencies.[92] It is likely that these concerns are related to feelings of greater visibility and marginalisation associated with being an indigenous minority, as discussed earlier in this chapter.[93]

5.56 There were also significant differences by age. Younger people (under 30) were less likely to be concerned about some of the scenarios concerning use of personal information by businesses, and about security of personal information on the internet, although a substantial majority of younger people were concerned about these things.[94] On the other hand, younger people were more likely to be concerned about compulsory ID numbers, employer monitoring of emails and employee drug testing.[95] Other significant factors for some questions were income and occupation.[96]

92 A majority of Māori (53 per cent) were "very concerned" about a compulsory ID number for every New Zealander, compared to 34 per cent of non-Māori.

93 In the US African-Americans are less likely than Whites to support the use of surveillance cameras and other forms of surveillance by government: Gandy, above n 50, 183; ABC News/*Washington Post* Poll "Surveillance Cameras Win Broad Support" (29 July 2007) Press Release http://abcnews.go.com (accessed 14 August 2007).

94 For example, 72 per cent of those aged under 30 were concerned about a business asking for personal information that does not seem relevant to the purpose of the transaction, compared to 88 per cent of those aged 30-59 and 85 per cent of those aged 60 + . Seventy-seven percent of those aged under 30 were concerned about the security of personal details on the internet, compared to between 84 and 90 per cent for those over 30.

95 Compulsory ID numbers: under 30, 55 per cent concerned; 45 + , 45 per cent concerned. Employer monitoring of emails: under 30, 63 per cent concerned; 30-44, 49 per cent concerned; 45-59, 52 per cent concerned; 60 + , 41 per cent concerned. Drug testing: under 30, 43 per cent concerned; over 30, 33-35 per cent concerned.

96 It is difficult to summarise variation by income and occupation, but for example those on lower incomes were generally more concerned about a compulsory ID number than those on higher incomes.

5.57 A survey of attitudes to privacy and consent issues in broadcasting was carried out for the BSA in 2003.[97] General findings of this survey included:

- 91 per cent of people agreed that "You would always want your own personal life to remain totally private", but 58 per cent agreed and 40 per cent disagreed that "New Zealand celebrities cannot complain when their personal life is shown on TV as it is part of being a celebrity".
- When asked to consider the balance between the right of television and radio to broadcast information about or pictures of individuals, and people's right to privacy, 37 per cent thought the balance was too strongly in favour of the broadcaster; 30 per cent thought it was about right; 8 per cent thought it was too strongly in favour of privacy; and 25 per cent thought they did not know enough to say.
- 39 per cent thought that they are sufficiently protected by New Zealand laws from the broadcasting of personal information about, or actual footage of, themselves; 25 per cent thought that they are not sufficiently protected; and 35 per cent felt that they had insufficient knowledge to form an opinion.

5.58 Another question in this survey asked about the acceptability of TV news or current affairs revealing various types of facts about a person who is standing for election for the city or district council. In order of acceptability, the facts were:

- academic qualifications (55 per cent thought this was acceptable);
- previous criminal conviction (45 per cent acceptable);
- history of mental illness (23 per cent acceptable);
- sexual orientation (15 per cent acceptable);
- financial history (14 per cent acceptable);
- extra-marital affair (11 per cent acceptable); and
- medical history (10 per cent acceptable).

Thus, some types of information appear to be more likely to be considered private than others. However, it is difficult to extrapolate from the answers to this question, as they are likely to be very dependent on the context and the way in which the question is phrased (for example, "financial history" is likely to elicit a different response than "history of bankruptcy").

5.59 In contrast to the OPC survey, Māori in the BSA survey were not always more concerned about privacy than non-Māori. For example, Māori were significantly more likely to find disclosure of information about an individual's medical history, history of mental illness and extra-marital affair acceptable. One possible explanation for this is that Māori may be more inclined to see some types of information as of interest to the wider community and not just the individual concerned. On the other hand, Māori were more likely than non-Māori to believe that, in relation to broadcasting of information and images, their privacy was not sufficiently protected by current laws. The BSA survey also found that men were generally more accepting than women, and younger people more accepting than older people, of the various scenarios of possible privacy intrusions that were presented to respondents.

97 Information about the BSA survey is from Broadcasting Standards Authority *Real Media, Real People*, above n 39, 89-124. The survey of 1195 people aged 15 and over was conducted by Colmar Brunton in February-March 2003 by means of face-to-face interviews. Fourteen per cent of those surveyed were Māori.

5.60 One issue which was not tested in the OPC or BSA surveys is relative levels of trust in different types of organisation with respect to handling of personal information. Focus group research conducted for the State Services Commission suggests that government organisations are considered more trustworthy than private sector organisations in relation to informational privacy, and that people trust some government departments more than others.[98] An opinion survey conducted for Statistics New Zealand produced similar results. When asked how comfortable they were providing information about themselves to various organisations, 51 per cent were comfortable providing information to Statistics New Zealand, 46 per cent to universities, 34 per cent to "the Government in general" and 31 per cent to market research companies. There were also different levels of trust in the handling of personal information by specific government departments, from 51 per cent confidence in the Ministry of Health to 29 per cent in Work and Income New Zealand.[99] It could be valuable to test these findings by including questions on the informational privacy trustworthiness of various organisations in surveys of public opinion on privacy, as has been done in other countries.[100]

5.61 It is difficult to draw firm conclusions from these surveys, but a number of overall points can be made about the opinion survey evidence:

- When asked in general terms about privacy, a majority of New Zealanders express concern about privacy, and a desire to keep their personal information private.
- However, more specific questions elicit a much wider range of responses. There are much higher levels of concern about some issues than others, with internet security and medical confidentiality ranking near the top and drug testing and video surveillance near the bottom for the population as a whole. Some types of personal information may also be more likely to be considered private than others, and some organisations appear to be trusted more than others to handle personal information appropriately.
- There is some divergence in attitudes between men and women, Māori and non-Māori, younger and older people, and people of different social classes. In some cases attitudes differ quite markedly, particularly between Māori and non-Māori.

CONCLUSION

5.62 Good law reform should be principled, not poll-driven. It should ideally be based on a reasoned response to the long-term needs of society, not quick fixes or reactions to passing panics. At the same time, the law cannot afford to get too far out of step with the values and attitudes of the society it serves. Reconciling these two considerations is one of the great challenges for law reform in general, and reform of privacy law in particular.

98 Reilly and Cullen, above n 26, 24-26, 55.

99 Statistics New Zealand/UMR Research *Public Attitudes to the Confidentiality, Privacy and Security of Official Government Survey Data*, above n 90, 13, 22-24.

100 See for example Perri 6 with Lasky and Fletcher, above n 80; Office of the Privacy Commissioner, Australia *Community Attitudes to Privacy 2007* (Office of the Privacy Commissioner, Sydney, 2007) 16-20.

5.63 What is clear from this chapter is that more research is needed into attitudes to privacy in New Zealand, including the history of privacy in this country, the influence of culture on attitudes, the views of New Zealand young people and the impact of new technologies on those views. Another important area for further research is relative levels of trust in different organisations with regard to privacy protection. It is worth exploring, too, whether there is a distinct "privacy culture" in New Zealand, shaped by our history, cultural makeup and small population size. The Law Commission is unable to conduct such research itself, but we hope that these topics may be taken up by researchers in universities and elsewhere.[101]

5.64 If nothing else, the study of attitudes to privacy can highlight the diversity of opinions on privacy issues within and between societies, and help to avoid simplistic assumptions or generalisations. The fact that different individuals and groups have such widely differing ideas about privacy creates particular difficulties in trying to frame laws that strike an appropriate balance for the society as a whole. The American writer E L Godkin, whose articles influenced Warren and Brandeis, wrote in 1890 that intrusion on privacy:[102]

> afflicts or annoys different persons in different degrees. It annoys women more than men, and some men very much more than others. To some persons it causes exquisite pain to have their private life laid bare to the world, others rather like it.

Godkin's words are just as true today. In the age of MySpace and mobile phones, reality television and reveal-all celebrity profiles, there is still a wide spectrum of opinion from those who shun the public gaze to those who cannot get enough of it.

101 A major research project looking at attitudes to health information privacy is currently under way at Massey University: Massey University "Who Should See our Health Records?" (11 June 2007) Press Release www.scoop.co.nz (accessed 12 June 2007).

102 E L Godkin "The Rights of the Citizen, – IV – To His Own Reputation" (July 1890) *Scribner's* 65, quoted in Seipp, above n 1, 89.

Chapter 6: Technology

6.1 Ever since Warren and Brandeis expressed concern that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'",[1] calls for greater legal and other protections for privacy have often been prompted by technological change. As we mentioned in chapter 1, the Law Commission's Review is in part a response to the major technological developments that have taken place since the passing of the Privacy Act 1993, in particular the rise of the internet. This chapter reviews these developments, and considers their implications for privacy and privacy-related law reform.

6.2 Following a brief discussion of the relationship between technology and society, we describe the extraordinary advances in computers in recent decades. These advances have profound implications for informational privacy, as does the rise of networked computing, and especially the development of the internet. Other technologies have implications not only for informational privacy but also for local privacy. We look particularly at technologies of surveillance and location-detection, and at technologies that identify and analyse the human body. All of these technologies have the potential to be used to invade or curtail privacy. However, technology may also provide means of protecting privacy, and we consider the role of privacy-enhancing technologies (PETs) in addressing privacy concerns. We conclude the chapter with some general thoughts on the implications of technological change for reform of the law of privacy.

6.3 This chapter is far from being an exhaustive survey of the technologies that may have implications, either positive or negative, for privacy. Our focus is on drawing out those implications as clearly as possible, without becoming too immersed in the technical details. The Commission claims no great technological expertise, and in the later stages of this Review we hope to hear more from those who are experts in this field.

TECHNOLOGY AND SOCIETY

6.4 The relationship between technology and privacy can be viewed as a subset of the wider question of the relationship between technology and society. It is possible to set up a simple opposition between theories of technology as an autonomous force, developing in ways that are independent of human direction,

1 Samuel D Warren and Louis D Brandeis "The Right to Privacy" (1890) 4 Harv L Rev 193, 195.

and approaches that see technology as shaped by society and politics.[2] However, Bennett and Raab conclude that "Most commentators see outcomes as shaped by a complex dynamic interaction between technology and society."[3] We are not prisoners of our technology, but nor are we fully its masters; in Ithiel Pool's words, "technology shapes the structure of the battle but not every outcome".[4]

6.5 Technologies are designed by people, and those people have particular aims. The aims of those who develop technologies are reflected in the capabilities and properties that are given to particular devices and systems. Although technologies may be used in ways their creators never intended, their in-built capabilities set limits to such uses. They are therefore shaped by social and political agendas at their creation, and may be further shaped by their users, but only within limits.

6.6 Technologies can be designed and used in ways that are more likely either to enhance privacy or to diminish it, and the law can help to shape technology in a more privacy-protective direction. However, there is often an understandable reluctance to engage in legal intervention at an early stage for fear of curbing developments that may be socially beneficial, and out of a concern to fully understand the implications of new technologies before regulating them. This can lead to a time-lag between the widespread adoption of new technologies and their regulation.[5] It can also mean that social norms in relation to a technology, including norms that are not supportive of privacy, may become so entrenched that it becomes difficult, if not impossible, for the law to intervene effectively.[6]

COMPUTERS AND DIGITAL DATA

Advances in computer technology

6.7 Concerns about the implications for privacy of the aggregation of personal information in computer databases first emerged in the late 1960s and early 1970s. Some of these early concerns are still very relevant today. The report of the New Zealand Law Revision Commission Sub-Committee on Computer Data Banks and Privacy, released in 1973, identified three key public concerns about storage of personal information in computer data banks: that the information might be "inaccurate, irrelevant, obsolete or slanted"; that the amalgamation of information from different sources might allow information to be used for purposes other than those for which it was originally provided; and that information could easily be disclosed without the consent or even the knowledge of the person to whom it related.[7] The report noted that:[8]

2 Colin J Bennett and Charles D Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge (Mass), 2006) 177-178; Gaia Bernstein "When New Technologies are Still New: Windows of Opportunity for Privacy Protection" (2006) 51 Vill L Rev 921, 929.

3 Bennett and Raab, above n 2, 178.

4 Ithiel de Sola Pool *Technologies of Freedom: On Free Speech in an Electronic Age* (Harvard University Press, Cambridge (Mass), 1983) 251, quoted in Bennett and Raab, above n 2, 178.

5 Martin Hirst and John Harrison *Communication and New Media: From Broadcast to Narrowcast* (Oxford University Press, South Melbourne, 2007) 282-283.

6 Bernstein, above n 2.

7 Law Revision Commission *Report of Sub-Committee on Computer Data Banks and Privacy* (1973) 17-18 (quoting the sub-committee's technical adviser, BAM Moon, Director of the Computer Centre, University of Canterbury).

8 Ibid, 18 (again quoting Mr Moon). For a similar but more recent view, see Daniel J Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2004) especially ch 6.

> One expression of opinion has been that the threat to the citizen is not so much in the invasion of his privacy per se but in the hold over the citizen which exists or might exist through having a source of information about him collated in a form that may be manipulated to his personal disadvantage.

6.8 While such views from an earlier phase of the information age still resonate strongly today, rapid advances in computer technology since the 1970s have created new privacy challenges and accentuated old ones. Information storage in computers of the 1960s and 1970s was highly centralised. Large mainframe computers were not connected to other computers, and were accessed by relatively few people. This is a far cry from today's world of ubiquitous, networked computing.

6.9 Today's computers are vastly more powerful than those that existed even a decade ago. A recent report from the National Academy of Sciences in the United States provides a useful summary of advances in computing, and their implications for privacy:[9]

- Computing power has increased exponentially, with a consequent decrease in the cost of computation. A standard desktop computer today is more powerful than the most expensive supercomputer of ten years ago, while an average cellphone today is at least as powerful as a personal computer from a decade before.
- Memory size has increased enormously, allowing for faster computation and making it possible to work on much larger data sets.
- Storage capacity has also vastly expanded, making possible the storage of data for long periods at little cost. Whereas data was previously discarded or reformatted as soon as possible in order to minimise storage costs, it is now more expensive to decide how to cull or transfer data to secondary storage than to keep it in primary storage. As a result, large amounts of raw data can be readily retrieved and analysed for new purposes, or aggregated with other data for further analysis.
- New forms of data can be stored. Some forms of data, such as high-quality video streams, were previously too large to be stored for long periods, but can now be kept in long-term storage. Data from a range of data-gathering devices (such as surveillance, tracking and biometric technologies discussed further below) is now available in digital form.
- Advances in software make it possible to analyse information in new and more powerful ways. It has become possible to discover previously unknown relationships among data elements. This, in turn, makes it easier to collate data about particular individuals, and to classify people into ever-more specific groupings.

6.10 According to the National Academy of Sciences report:[10]

> The end result of the improvements in both the speed of computational hardware and the efficiency of the software that is run on that hardware is that tasks that were unthinkable only a short time ago are now possible on low-cost, commodity hardware running commercially available software. Some of these new tasks involve the extraction of information about the individual from data gathered from a variety of

9 National Research Council of the National Academies *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washington, DC, 2007) 88-97.

10 Ibid, 97.

> sources. A concern from the privacy point of view is that – given the extent of the ability to aggregate, correlate, and extract new information from seemingly innocuous information – it is now difficult to know what activities will in fact compromise the privacy of an individual.

6.11 The effects of dramatic increases in the capabilities of computer hardware and software are multiplied further by greatly increased connectivity between computers, as well as between computers and other types of information and communications technologies. We discuss in the next section the most significant example of networking, the internet, but here we note some general points about the rapid growth in connectivity:[11]

- Computers connected to a network are not limited by their own capacities, but can make use of the power of other computers in the network.
- Users of networked computers can gain access to information gathered by, or stored on, another machine on the same network without touching or being in the same place as that machine.
- The quantity of data that can be transferred over a network in a given time ("bandwidth") is increasing dramatically.

6.12 The National Academy of Sciences report concludes that:[12]

> From the privacy point of view, interconnectivity seems to promise a world in which any information can be accessed from anywhere at any time, along with the computational capabilities to analyze the data in any way imaginable.

Moreover:[13]

> Once stored, data are potentially available for analysis by any computer connected via a network to that storage. Networked computers can share any information that they have, and can aggregate information held by them separately. Thus it is possible not only to see all of the information gathered about an individual, but also to aggregate the information gathered in various places on the network into a larger view of the activities of that individual.

Data collection and analysis

6.13 These advances in computing have made it possible to extract and analyse data in ways that have very significant implications for informational privacy. Some of these techniques are not new, but they are made easier by more powerful computer technology. Two key techniques, used by both public – and private – sector organisations, are data matching and data mining. *Data matching* involves comparing data that comes from different sources, and has been collected for different purposes. The aim is generally to find data that relates to the same person, and it is commonly used for purposes such as detecting errors or fraud, locating particular individuals, and determining eligibility for government benefits. *Data mining* involves extracting information that is implicit in data sets, usually by discovering new relationships among data elements.[14]

11 Ibid, 97-100.

12 Ibid, 99.

13 Ibid, 101.

14 Ibid, 95.

6.14 Both data matching and data mining can raise privacy concerns because:[15]

- they involve the use of personal data for purposes other than those for which it was collected;
- they seek to uncover previously unknown information about people;
- they can occur without the knowledge or consent of the data subject;
- errors or incomplete information in the original data can be repeated and their effects multiplied; and
- they generally involve automated processing, and may involve automated decision-making, removing the element of human judgement.

6.15 Data collection and aggregation are also facilitated by computer technology. In particular, it is possible for private companies to amass a much greater quantity of information about individuals than ever before, with the aim of more accurately profiling consumers.[16] In Daniel Solove's vivid phrase, "data is the perspiration of the Information Age".[17] Our everyday transactions – including use of credit cards, bank cards, loyalty cards, mobile and other phones, and the internet – leave a trail of digital data that companies can use to gain a more detailed understanding of their customers. Such data can also be combined with publicly-available information, such as censuses and information from public registers. As we discuss in our *Public Registers* issues paper, information on public registers has increasingly been digitised, making it easy to access and download in bulk.[18]

6.16 In the United States, personal information companies that collect personal data from a range of sources and sell it to marketers have annual revenues in the billions of dollars. The largest of these companies have information on more than half the US population.[19] In New Zealand, however, most companies' data-gathering activities appear to be limited to collecting information about their own customers, and often combining it with publicly-available information.[20] On-selling of information to third parties is regulated by the Privacy Act and, in many cases, restricted by companies' own privacy policies.

6.17 Advances in computer technology make it possible for vast quantities of data about individuals to be collected, stored, combined and analysed. Marketers use this information to develop profiles of particular types of consumers, and even of individuals. This allows them to target their marketing to more specific groups, in order to decrease costs and increase response rates. It can be argued that this is economically efficient, bringing "lower prices and more choices

15 Australian Law Reform Commission *Review of Australian Privacy Law* (ALRC DP72, Sydney, 2007) 325-327; Office of the Privacy Commissioner "Data matching – Overview" www.privacy.org.nz (accessed 19 September 2007).

16 Solove *The Digital Person*, above n 8, 16-21; Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006) 20-21; National Research Council of the National Academies, above n 9, 196-200; Kris Herbert "Digital Tracks: Your Information Thumbprint in Cyberspace" (January/February 2007) *New Zealand Geographic* 64.

17 Solove *The Digital Person*, above n 8, 19.

18 New Zealand Law Commission *Public Registers: Review of the Law of Privacy: Stage 2* [NZLC *Public Registers*] (NZLC IP3, Wellington, 2007) 10-12, 61-62.

19 Solove *The Digital Person*, above n 8, 19-20.

20 The main exceptions are credit reporting companies, which collect personal information from banks, retailers and other credit providers, and sell that information (in the form of credit reports) to third parties.

for consumers".[21] On the other hand, it is likely that most consumers have little idea of the detailed profiles that can be built up about them. Consumers may believe that information has been provided for a particular purpose (such as receiving discounts through loyalty schemes), but it may also be used for other purposes, and combined with other data without their knowledge.[22] They are therefore likely to have little say about the way in which their personal information is used. This may be considered problematic from a privacy perspective.

6.18 Companies also collect personal information for the purpose of protecting intellectual property rights. Digital Rights Management (DRM) technologies have been developed because digital content (including text, images and sound) can be freely and perfectly copied. Copyright owners therefore use DRM technologies to protect their rights in such content by imposing limits on the ways in which digital material can be accessed, used, copied and distributed. In doing so, however, DRM technologies often collect personal information about the users of copyright digital content, and track their use of the material (when, how often, and for how long they use it, for example). Privacy advocates have expressed concern about such data collection, and particularly about the potential for information collected in this way to be used for other purposes such as marketing.[23]

THE INTERNET

6.19 When New Zealand's Privacy Act was passed, the internet (and, more particularly, the World Wide Web) was in its infancy. Since then, it has transformed many aspects of our lives. It has also given rise to new and difficult privacy issues, which we outline in this section. We have already discussed in chapter 5 the ways in which the internet may be affecting young people's attitudes to privacy. In chapter 7 we will consider the difficulties created from a legal standpoint as a result of the transnational nature of the internet.

6.20 We have referred above to the networking of computers, and the increased capacity and accessibility that this creates. The internet is a type of super-network, "a worldwide collection of interconnected computer networks based on a set of standard communication protocols".[24] Through the internet, users can access the World Wide Web, a collection of linked electronic documents and files.

21 Declan McCullagh "Database Nation: The Upside of 'Zero Privacy'" (June 2004) *Reason* www.reason.com (accessed 19 October 2006).

22 In a 2006 public opinion survey, 89 per cent of respondents expressed concern about a scenario in which "You supply your information to a business for a specific purpose and the business uses it for another purpose": Privacy Commissioner/UMR Research *A Summary Report* (2006) 11, available at www.privacy.org.nz.

23 Lindy Siegert, Technology Team Leader, Office of the Privacy Commissioner "Digital Rights Management (DRM) Technology and Privacy" (background to comments made to an Agencies Leaders' Forum meeting at the State Services Commission, 23 March 2005); David Lindsay and Sam Ricketson "Copyright, Privacy and Digital Rights Management (DRM)" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 121; Australian Law Reform Commission *Review of Australian Privacy Law*, above n 15, 339-340; National Research Council of the National Academies, above n 9, 99-100; Rafael Ruffolo "Study Says DRM Violates Canadian Privacy Law" (20 September 2007) *PC World* www.pcworld.com (accessed 21 September 2007).

24 Australian Law Reform Commission *Review of Australian Privacy Law*, above n 15, 315.

6.21 The internet has a number of notable characteristics:

- It has no borders – it is not located in any one state, and is accessible from anywhere (subject to the necessary technological systems for connecting to it, and to any steps that governments or others may take to block or filter content).
- It is not centrally owned or controlled.
- It operates in such a way as to make it difficult to control or trace the flow of data.[25]
- It is interactive and dynamic – Web content is continually being added or modified, and it has become increasingly easy for anyone with access to the internet to create their own websites or contribute to existing ones.
- While the content of the Web constantly changes, it is also persistent – that is, information that was once on a website can be searched for and retrieved even after the content of the site has been changed.

6.22 The internet is now widely used and accessible in New Zealand. In 2006, nearly two-thirds of households had access to the internet at home, and there were some 1.4 million internet subscribers (including businesses and government). Sixty-nine per cent of people over 15 had used the internet at some stage during the year, and young people were more likely to have used the internet than older people. The most common activities on the internet were emailing, general Web surfing or browsing, internet banking, searching for information on goods and services, and listening to music.[26]

6.23 It is not possible here to review all of the potential privacy implications of the internet.[27] We focus on two broad themes: the collection of personal information by companies that track and record users' online activities, and the online availability of personal information posted by private individuals. We exclude from consideration issues that are more properly considered questions of internet security, such as use of the internet by computer "hackers" to gain unauthorised access to information. Security breaches can clearly lead to breaches of informational privacy, and effective security is in many cases an essential prerequisite to the protection of privacy. However, we consider that this issue is sufficiently distinct from privacy that we do not discuss it here.[28]

---

25 For an explanation of the design features of the internet that make this so, see House of Lords Science and Technology Committee "Personal Internet Security. Volume 1: Report" (HL Paper 165-I, 2007) 10-13.

26 Margie Comrie, Franco Vaccarino, Susan Fountaine and Bronwyn Watson *Media Literacy Information in New Zealand: A Comparative Assessment of Current Data in Relation to Adults* (Broadcasting Standards Authority, Wellington, 2007) 41-51. A recent survey of New Zealanders' internet use is Allan Bell, Charles Crothers, Andy Gibson, Ian Goodwin, Karishma Kripalani, Kevin Sherman and Phillipa Smith *New Zealanders and the Internet: A Preliminary Profile of Usage and Attitudes* (2007 Benchmark Survey: Interim Report, World Internet Project New Zealand, Institute of Culture, Discourse and Communication, AUT University, Auckland, December 2007).

27 One issue not reviewed here, but which is likely to become more prominent in future, is privacy in "massively multi-player online role-playing games" and virtual worlds such as Second Life: see Tal Z Zarsky "Information Privacy in Virtual Worlds: Identifying Unique Concerns Beyond the Online and Offline Worlds" (2004) 49 NYL Sch L Rev 231. On wider legal issues in virtual worlds see Kevin W Saunders "Virtual Worlds – Real Courts" (2007) 52 Vill L Rev 187; Scott Holdaway "I Don't Know the Name, but the Avatar Sure Rings a Bell…: An Analysis of the Law Relevant to the Appearance of Representations of Personality in Cyberspace" (2007) 13 Canta LR 1.

28 For a brief review of internet security issues see Australian Law Reform Commission, above n 15, 319-320; for a more detailed discussion see House of Lords Science and Technology Committee, above n 25.

Collection of personal information online

6.24 There is an abundance of personal information that can be collected by companies and other organisations via the internet. This is done both openly and secretly. Overt collection of data takes place, for example, when users are asked to register with a particular website.[29] They may be required to register in order to view particular content, or in order to engage in particular activities, such as online purchasing. When registering, they may be asked to provide certain personal information, such as name, sex, age, place of residence and income, as well as personal preferences (for example, an online bookstore might ask about what kinds of books a user likes to read). In addition, once a person has registered, the website may keep track of their transactions and make this information available for the user to view. For example, users of an online bookstore could view their past purchases, and the website could also use the pattern of past purchases to recommend other books that might be of interest.

6.25 Of greater concern from a privacy perspective is the collection of information without the user's knowledge or consent. Daniel Solove explains that:[30]

> When a person explores a website, the website can record data about her ISP [Internet Service Provider], computer hardware and software, the website she linked from, and exactly what parts of the website she explored and for how long. This information is referred to as "clickstream data" because it is a trail of how a user navigates throughout the web by clicking on various links. It enables the website to calculate how many times it has been visited and what parts are most popular…. Due to the interactive nature of the Internet, marketers can learn how we respond to what we hear and see. A website collects information about the way a user interacts with the site and stores the information in its database. This information will enable the website to learn about the interests of a user so it can better target advertisements to the user.

The information collected in this way is generally linked to a particular computer rather than to an identifiable individual. Computers are identified by their IP (Internet Protocol) address, a number assigned by the user's Internet Service Provider. However, if the person using the computer has registered with a particular site, the information can be linked to that individual.[31]

Search companies

6.26 Internet search companies also collect information every time a user conducts a search. This information includes the search terms typed in by the user (the query), the IP address of the user's computer, and a unique identifier for

29 Solove *The Digital Person*, above n 8, 23.

30 Ibid, 23-24. For an explanation of how "cookies", "web bugs" and "spyware" collect information about internet users see ibid, 24-25; Australian Law Reform Commission, above n 15, 317-318.

31 IP addresses will be changing with the implementation of a new internet platform known as Internet Protocol version 6 (IPv6), replacing the current IPv4. New Zealand appears to be progressing slowly on the transition to IPv6. It seems likely that IPv6 will have some significant implications, both positive and negative, for online privacy. See Michael W Hubbard "Internet Protocol Version 6: Data Security and Privacy Concerns with the New Internet" (September 2007) *The Federal Lawyer* United States 34. On IPv6 in New Zealand see Stuart Corner "New Zealand Takes First Steps to IPv6" (13 June 2007) www.itwire.com (accessed 29 November 2007); and the website www.ipv6.org.nz.

the user's web browser. Such information is stored by the search companies, who say that search logs are used to monitor and improve the functioning of their search engines. They are also used for targeted advertising, discussed below.[32]

6.27 If users have accounts with the search companies, for which users provide personally-identifying information, the account information is held separately from search information by all the major companies. However, there are concerns about the possibility of linking these two sets of information. Another concern is that, as large search companies now offer a range of services (including email, maps and instant messaging), they may be able to combine information from these different sources, including in ways that allow information to be linked to individuals.[33] Furthermore, even though personally-identifying information is not usually kept in search logs, the content of the searches themselves may make it possible to link them to individuals. This became clear when search company America Online briefly made the search records of some 658,000 people over a three-month period available on the internet for researchers. Although the records were anonymised, media organisations were able to trace some users and identify them by name.[34]

6.28 Search companies have come under increasing pressure to limit their retention of search information, and the major companies have recently announced a range of steps that they will be taking to protect the privacy of this information. These steps vary between companies, but include partially or completely removing IP address information; filtering personally-identifying search terms (such as names, addresses and phone numbers) out of queries; and allowing users to choose to have their search information deleted within hours of the search. With the exception of the last-mentioned approach, the search data will be removed between 13 and 18 months after the search, depending on the company.[35]

Targeted advertising

6.29 Advertising makes it possible for search engines and other website services to be made available for free. Some people consider, however, that there is a privacy cost to users as a result of the methods used by websites to target advertisements to particular individuals. A simple form of targeted advertising is employed by Google's AdSense programme, which displays advertisements based on the particular search terms entered by a user.[36] More complex methods known as "behavioural targeting" involve targeting advertisements to individual users based on their longer-term search or browsing history, as well as any other information about them that may have been collected (such as age, sex, geographic location and occupation). It can involve the use of clickstream data, "following" users as they

32 Center for Democracy & Technology *Search Privacy Practices: A Work in Progress* (Washington, DC, 2007) 1.

33 Ibid, 3. On the privacy policies of the web mail services provided by three major companies that also provide search engines, see Erik Larkin "Who Best Safeguards the Privacy of Your Web Mail?" (26 September 2007) *PC World* www.pcworld.com (accessed 28 September 2007).

34 National Research Council of the National Academies, above n 9, 105-106.

35 Center for Democracy & Technology, above n 32, 2-4.

36 These advertisements have been based on the terms entered in each individual search, but Google has been looking at basing advertisements on the pattern of terms that emerges in a given search session: Eric Auchard "Google Wary of Behavioral Targeting in Online Ads" (31 July 2007) www.reuters.com (accessed 1 October 2007).

visit different websites and tracking their interactions with those sites: how long they stay at particular sites, which advertisements they click on, and what purchases they make, for example.[37] Social networking sites have also developed ways of targeting advertisements to their users based on information in users' online profiles, or on alerting a user's online "friends" to that person's purchases or other activities on participating third-party websites.[38]

6.30 Some users of the internet are unconcerned about targeted advertisements, and may even welcome information about products or services that relate to their particular interests. For others, the mere fact of receiving targeted advertisements may feel like an invasion of their privacy: it may feel as though someone is spying on their online activities to learn about their tastes and interests. While the process of customising advertisements is automated, so there is no actual person looking over the shoulders of internet users, the tracking of clickstream data can be seen as "ad-stalking".[39] A number of privacy advocacy groups in the United States have called for the creation of a "Do Not Track List", which would make it easier for internet users to opt out of online tracking by advertisers.[40] Even where clickstream data is not used, behavioural targeting involves the collection, storage and use of personal information in ways that many internet users may not be aware of, and this is of concern to privacy advocates.[41]

Availability of personal information online

6.31 We have discussed above the collection of personal information online by companies and others, and the privacy concerns that this raises. Other privacy concerns relate to the increasing amount of personal information that is accessible on the internet. We discuss in our *Public Registers* issues paper the online availability of some personal information held in public registers, and we have

37 Megan Tady "Marketers Still Free to Stalk Consumers Online" (27 November 2006) http://newstandardnews.net (accessed 1 December 2006); William Marra "Yahoo's SmartAd Raises Privacy Concerns" (4 July 2007) www.abcnews.go.com (accessed 6 July 2007); Center for Democracy and Technology "Privacy Initiatives Key to Addressing Behavioral Targeting Concerns" (8 August 2007) Policy Post 13.11 www.cdt.org (accessed 9 August 2007); Center for Digital Democracy and United States Public Interest Research Group "Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices" (1 November 2007).

38 Jonathan Richards "Social Networks Get Personal with 'Hyper-Targeting'" (5 November 2007) *The Times* http://technology.timesonline.co.uk (accessed 6 November 2007); Louise Story "Facebook is Marketing Your Brand Preferences (With Your Permission)" (7 November 2007) *New York Times* www.nytimes.com (accessed 8 November 2007); Catherine Holahan "Facebook May Scale Back Beacon" (28 November 2007) *BusinessWeek* www.businessweek.com (accessed 29 November 2007); Louise Story and Brad Stone "Facebook Retreats on Online Tracking" (30 November 2007) *New York Times* www.nytimes.com (accessed 3 December 2007).

39 Lara Sinclair "Ad Systems Threaten Privacy" (2 August 2007) *The Australian IT* www.australianit.news.com.au (accessed 3 August 2007).

40 Center for Democracy and Technology and others, submission to the United States Federal Trade Commission (FTC) in advance of the FTC Town Hall meeting on "Behavioral Advertising: Tracking, Targeting, and Technology", Washington, DC, 1-2 November 2007. See also Louise Story "Consumer Advocates Seek a 'Do-Not-Track' List" (31 October 2007) *New York Times* www.nytimes.com (accessed 2 November 2007); Ryan Singel "Privacy Groups Ask for Online 'Do Not Track' List" (31 October 2007) www.wired.com (accessed 29 November 2007); Jonathan Weber "Putting a Price on Privacy" (5 November 2007) *The Times* http://technology.timesonline.co.uk (accessed 6 November 2007); Thomas Claburn "Privacy vs Personalization: Can Advertisers Ward Off Looming Threat of Do Not Track List" (10 November 2007) *Information Week* www.informationweek.com (accessed 12 November 2007).

41 Center for Democracy and Technology "Privacy Initiatives Key to Addressing Behavioral Targeting Concerns", above n 37.

discussed the privacy implications of online access to court records in an earlier report.[42] Here we are concerned mainly with the posting of various forms of personal information (particularly images) on the internet by private individuals. This creates some major challenges for the protection of informational privacy.

6.32 In chapter 5 we looked at the phenomena of blogging and social networking, and the apparent willingness of young people in particular to post significant amounts of personal information on such websites. Concerns have been raised about the potential for information that people post about themselves online to be misused by identity thieves, blackmailers and sexual predators, or for embarrassing material to be viewed by current or future employers or university authorities.[43] Journalists have also started turning to social networking sites for source material, which may raise ethical questions when young people's online comments that are not intended for a general audience are quoted in the media.[44]

6.33 Of greater privacy concern, however, and more likely to raise questions of legal liability, is the online posting of information about others without their consent. Blogs and social networking sites are again of particular concern in this respect. In writing about their own lives, people also write about, or post photos or videos of, their friends, lovers, families and acquaintances. Those other people may not always be aware that material about them has been posted, and are unlikely to have given their consent. When they become aware that information about them is accessible on the internet, they may feel that their privacy has been invaded.[45]

6.34 Another development that is causing concern to privacy advocates is the emergence of websites that create profiles of people by searching the Web for information about a person and bringing it together in one place. Online social networks are a particularly valuable source of such information. Profiling sites create profiles without the knowledge or consent of the subject of the profile, and may contain information that is embarrassing or incorrect. Some of these sites allow people to request that information about them be corrected or deleted. However, there is unlikely to be any legal recourse for people who object to their profiles, since all the information is obtained from publicly-available websites.[46]

---

42 NZLC *Public Registers*, above n 18, – see 33, fn 62 for some figures about the online availability of public registers; New Zealand Law Commission *Access to Court Records* (NZLC R93, Wellington, 2006) ch 6.

43 See for example Ed Pilkington "Blackmail Claim Stirs Fears over Facebook" (16 July 2007) *The Guardian* www.guardian.co.uk (accessed 16 July 2007); Alice Hudson "Teenage Girls Posting 'Dangerous' Photos Online" (7 October 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 9 October 2007); Keri Welham "'I Lov Animals and Im a Total Boy Magnet': What Your Children are Posting on the Internet" (27 October 2007) *Dominion Post* Wellington E7; Fiona Smith "Mind Who's Watching" (21 November 2007) *The Press* Christchurch C1; Australian Law Reform Commission, above n 15, 1728-1731; Daniel J Solove *The Future of Reputation: Gossip, Rumour, and Privacy on the Internet* (Yale University Press, New Haven, 2007) 38; European Network and Information Security Agency *Security Issues and Recommendations for Online Social Networks* (ENISA Position Paper 1, 2007).

44 See for example Elizabeth Binning "Police Probe Murder Claims on Bebo" (11 September 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 1 October 2007); Colin Espiner "English to See Lawyers Over Gay Website's Attack on Son" (26 September 2007) *The Press* Christchurch www.stuff.co.nz (accessed 1 October 2007); discussion on Radio New Zealand National "Mediawatch" programme, 23 September 2007.

45 Ashley Hurst "Is the Writing on the Wall for Facebook?" (2 July 2007) *The Guardian* www.guardian.co.uk (accessed 1 October 2007); Solove *The Future of Reputation*, above n 43, ch 3.

46 Anita Hamilton "Online Snooping Gets Creepy" (2 August 2007) *Time* www.time.com (accessed 4 August 2007); Stefanie Olsen "At Rapleaf, Your Personals are Public" (31 August 2007) and "People Search Engine Rapleaf Revises Privacy Policy" (4 September 2007) www.news.com (accessed 28 September 2007).

Images on the internet

6.35 The online posting of photographs and videos is a matter of particular concern. When Warren and Brandeis wrote that instantaneous photography was invading private life, and that a legal remedy was required for "the unauthorized circulation of portraits of private persons",[47] they could scarcely have imagined the even greater ease with which images of people could be circulated in the internet age. Digital photography and camera phones have made it easy to take numerous photographs and upload them to the Web, sometimes without the knowledge of the subject. Photo-sharing sites such as Flickr and video-sharing sites such as YouTube have made images of individuals accessible to a worldwide audience. Social networking sites also include many photographs and video clips, with varying degrees of public access. Once images have been posted on the internet it becomes difficult, if not impossible, to control them or have them removed.

6.36 The availability of images of people on the internet gives rise to privacy fears because such images can so easily be:

- disseminated widely and viewed by many people;
- stored permanently and viewed repeatedly, providing "opportunity for ongoing objectification of the subject, and therefore ongoing harm";[48]
- subject to close scrutiny (using "zoom" and other features); and
- taken out of context and given new meanings, including embarrassing, derogatory or sexualised meanings.

6.37 Concerns about posting of photographs and videos on the internet have generally focused on those that have been taken without authorisation and/or are intimate in nature.[49] However, even where there is nothing in the image itself that is intimate or embarrassing, images can be recontextualised in ways that may cause distress or embarrassment. Two recent stories from the United States illustrate the way in which an innocent image can be given new meaning by being put in a different context, and the difficulty of controlling images once they have been posted on the Web.

6.38 In the first story a photograph of a female high school athlete was posted, together with ribald comments, on a popular sports comedy blog. The photo was quickly copied or linked to by other sites. Within a very short space of time an unofficial website and a MySpace page had been created by "fans" of the young woman, along with a fake profile on Facebook, and a short video of her posted on YouTube had been viewed 150,000 times. The subject of this unwanted attention reported feeling violated and demeaned by the theft and commodification of her image. However, while the fake Facebook profile was taken down at her request, the woman and her family concluded that there was little they could do to control the proliferation of material about her on the internet.[50] In the second story a photograph of a 15-year-old girl taken by her church counsellor and posted on the Flickr website was used in an

47 Warren and Brandeis, above n 1, 195.

48 Standing Committee of Attorneys-General (Australia) *Unauthorised Photographs on the Internet and Ancillary Privacy Issues* (Discussion Paper, 2005) 13.

49 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004); Standing Committee of Attorneys-General, above n 48.

50 Eli Saslow "Teen Tests Internet's Lewd Track Record" (29 May 2007) *Washington Post* www.washingtonpost.com (accessed 5 June 2007).

advertisement by a company in Australia accompanied by a mocking slogan. The girl and her family are suing the company for invasion of privacy and libel, alleging that its actions have caused her humiliation and mental anguish.[51]

6.39 Other concerns about images on the internet relate to online mapping services. These concerns arose originally with websites providing bird's-eye views of locations, and allowing users to focus in so that individual houses can be viewed from above. More recently, even greater privacy concerns have been raised about Google's Street View service, which provides 360-degree views from street level. Street Views of a number of United States cities are already available, and the service is to be extended to other countries, including Australia. Street View allows individual people to be seen, sometimes in embarrassing locations or poses. Google has promised that it will obscure faces and car number plates on request, and will comply with local privacy laws as Street View is extended to other countries. Moreover, the images on such sites are photographs which may be several years old, rather than real-time images. Nevertheless, concerns remain about whether Google will in fact comply with, and accept liability under, local privacy laws. There is also potential for such services to become more intrusive in future by, for example, using real-time images or combining images with other information.[52]

6.40 Privacy concerns about photographs on the internet may be accentuated by the development of facial-recognition search engines. While it is already possible to search the internet for images, these have been located using captions or other nearby text – it has not been possible to search the images themselves. New programmes, however, aim to directly match images of people on the internet based on the shape of their faces and other features. This means that if a user finds an image of a person on the internet, he or she can search the entire Web for other images of that person. In addition, photographs can be "tagged" with names and other details, so it may become possible to find out the identity of a person in a photo by matching it with a tagged image. At present the accuracy of image-based search engines is open to question, but the potential for such services to remove the anonymity of online photographs of individuals is of concern to privacy advocates.[53]

---

51 Noam Cohen "Use My Photo? Not Without Permission" (1 October 2007) *New York Times* www.nytimes.com (accessed 2 October 2007); Plaintiff's Original Petition, *Chang v Virgin Mobile*, District Court, Dallas County, Texas, posted in Lawrence Lessig "On the Texas Suit Against Virgin and Creative Commons" (22 September 2007) www.lessig.org/blog (accessed 2 October 2007).

52 "Cyber Travel Gets Up Close and Personal" (31 May 2007) *New Zealand Herald* Auckland; Miguel Helft "Google Zooms in Too Close for Some" (1 June 2007) *The New York Times* www.nytimes.com (accessed 5 June 2007); Stephen Hutcheon "Smile, You're on Google's Candid Camera" (4 June 2007) *The Sydney Morning Herald* www.smh.com.au (accessed 3 October 2007); Peter Griffin "Cyberlife Becomes a Road Movie" (7 June 2007) *New Zealand Herald* Auckland; S James Snyder "Google Maps: An Invasion of Privacy?" (12 June 2007) *Time* www.time.com (accessed 13 June 2007); "The World on Your Desktop" (8 September 2007) *The Economist Technology Quarterly* 14; Terry Pedwell "Google's New Street-Level View Concerns Privacy Commissioner" (12 September 2007) *The Globe and Mail* Toronto www.theglobeandmail.com (accessed 13 September 2007); Peter Fleischer (Google Global Privacy Counsel) "Street View and Privacy" (24 September 2007) http://google-latlong.blogspot.com (accessed 25 September 2007); Darren Osborne "Smile! You're on Google's Camera" (23 November 2007) www.news.com.au (accessed 26 November 2007); "Google's Candid Camera Snaps Australia" (24 November 2007) www.stuff.co.nz (accessed 26 November 2007).

53 Tom Simonite "Face-Hunting Software Will Scour Web for Targets" (19 December 2006) *New Scientist* www.newscientist.com (accessed 8 January 2007); Mason Inman "Face Recognition for Online Photo Searches Sparks Privacy Fears" (5 January 2007) http://news.nationalgeographic.com (accessed 3 October 2007); Note "In the Face of Danger: Facial Recognition and the Limits of Privacy Law" (2007) 120 Harv L Rev 1870.

Implications for privacy law

6.41 There are a number of legal issues relating to the impact of the internet on privacy that appear to warrant further consideration. These include overarching issues of jurisdiction and enforceability of decisions that are not specific to privacy, but have important implications for it. Jurisdictional issues, which are discussed further in chapter 7, arise from the fact that the internet has no borders and can be accessed anywhere in the world. A webpage could be uploaded in one country, hosted on a server located in a second country, and downloaded in a third country. In which state(s), then, would a person be able to bring an action or lay a complaint for breach of privacy in relation to material on the webpage? What effect, if any, could a decision in one jurisdiction have on the other jurisdictions?[54]

6.42 There are also questions about *who* is liable for material on the internet that is seen as breaching privacy. What are the respective liabilities, if any, of the person who posted the material on a webpage, people who link to that page from other webpages, the internet service provider, and the providers of other online services (such as blog providers or social networking sites)?[55]

6.43 Other issues relate more specifically to the terms of the Privacy Act 1993:

- The information privacy principles (IPPs) set out in the Act do not apply in respect of personal information collected or held by an individual "solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs" (section 56). Consider a situation in which A writes about, or posts pictures of, B in a blog or online social network page primarily concerned with A's personal affairs. It seems likely that the Privacy Act will not apply in such a case, even though there may have been a significant interference with B's privacy.
- The Act and the IPPs protect "personal information", defined as information about an identifiable individual.[56] This would appear to exclude information gathered about an IP address, which relates to a computer not a person. As discussed above, companies are able to gather extensive information about particular IP addresses. While this information may not be directly "about" an identifiable individual, it is often very personal in nature, and it may be possible to link the address to a person.
- The IPPs relating to the source of personal information, and to use and disclosure of personal information, do not apply to information contained in, or sourced from, a "publicly available publication".[57] The latter phrase is

54 Dan Jerker B Svantesson "Protecting Privacy on the 'Borderless' Internet – Some Thoughts on Extraterritoriality and Transborder Data Flow" (2007) 19 Bond LR 168; Damien O'Brien "Blogs and the Law: Key Legal Issues for the Blogosphere" (2007) 12 MALR 141, 156-158; David Harvey *internet.law.nz: selected issues* (LexisNexis, Wellington, 2005) ch 2.

55 Judit Bayer has researched questions relating to the liability of internet service providers for third-party content, and has a forthcoming article on this topic in the Victoria University of Wellington Law Review – an extract and table of contents are available at www.policy.hu/bayer (accessed 28 November 2007). Online liability questions in the context of the United States are discussed in Solove *The Future of Reputation*, above n 43, 149-159.

56 Privacy Act 1993, s 2(1), definition of "personal information".

57 Privacy Act 1993, s 2(1), definitions of "publicly available information" and "publicly available publication"; s 6, Principles 2, 10, 11.

defined as meaning "a magazine, book, newspaper, or other publication that is or will be generally available to members of the public; and includes a public register". There may be issues about the application of this exemption to material published on the internet. Issues may also arise concerning the application of the exclusion of news media from the definition of "agency" where news and current affairs websites are concerned.[58]

- Non-compliance with certain IPPs is permissible when it has been "authorised" by the individual concerned.[59] This means that an agency can, for example, use personal information for a purpose other than that for which it was obtained, or disclose personal information to a third party, with the consent of the individual concerned. However, authorisation or consent may have little meaning on the internet. Website privacy policies may state that, by visiting the site, a user is assumed to have accepted the information-handling practices set out in the policy. Few users read or understand the often-complex privacy policies.[60]

We will examine issues such as these, and other specific implications of the internet for privacy law, in more detail in the later stages of the Review.

SURVEILLANCE AND LOCATION TECHNOLOGIES

6.44 Privacy reviews in the past have considered the potential impact of earlier generations of surveillance technologies.[61] On the verge of a quantum leap from "old surveillance" to the "new surveillance,"[62] it is timely for this Review to reconsider surveillance technologies. The new surveillance is projected to "transform surveillance from a conscious decision by specific corporate or governmental actors into a constant, inadvertent activity by virtually everyone."[63] These technologies offer many potential benefits and efficiencies to society and to individual citizens. However, there is an issue as to whether use of these technologies will be to the cost of both informational and local privacy. Privacy advocates have warned that Western society is on the verge of becoming a "wholesale surveillance society". On one prediction, there will be no place on earth where an ordinary person will be able to avoid surveillance.[64] In this section we review some of the key trends and technological developments that could have a significant impact on privacy.

58 Privacy Act 1993, s 2(1), definitions of "agency", "news activity" and "news medium".

59 Privacy Act 1993, s 6, Principles 2, 3, 10 and 11.

60 Research in the United States has found significant levels of misunderstanding of privacy policies, including a mistaken belief that, if a website has a privacy policy, the website will not share personal information with other websites or companies: Joseph Turow, Deirdre K Mulligan and Chris Jay Hoofnagle *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace* (Annenberg Public Policy Center, University of Pennsylvania/Samuelson Law, Technology & Public Policy Clinic, University of California, Berkeley, 2007).

61 See, for example, consideration of "electronic and optical extensions of the human senses" in the report of the Younger Committee: Report of the Committee on Privacy (1972) Cmnd 5012, 153.

62 A term used in the work of Gary T Marx; see for example Gary T Marx "Ethics for the New Surveillance" (1998) 14 The Information Society 171; Gary T Marx "What's New About the 'New' Surveillance?" (2005) 1 Surveillance & Society 9.

63 Kevin Werbach "Sensors and Sensibility" (2007) 28 Cardozo L Rev 2321.

64 A Michael Froomkin "The Death of Privacy?" (2000) 52 Stan L Rev 1461, 1476. See also Kevin D Haggerty and Richard V Ericson "The Surveillant Assemblage" in Clive Norris and Dean Wilson (eds) *Surveillance, Crime and Social Control* (Ashgate, Aldershot, 2006) 75, discussing the "disappearance of disappearance"; Surveillance Studies Network, above n 16, 49-75.

Key trends

6.45 A number of technological developments in computing, telecommunications, photography, and sensing technologies have converged to produce the "new surveillance:"[65]

> Compared to the 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.

6.46 Fibre optic technology allows the rapid transmission of huge amounts of data over long distances; developments in photography allow images to be captured digitally; and developments in storage and processing allow for quick and cheap retrieval and analysis.[66] Developments in sensing technologies have created devices that enable the collection of information about people, their movements, their transactions and their daily lives. Devices are routinely easy to use and are becoming smaller, cheaper and less noticeable all the time.

6.47 Significant developments in the applications of surveillance technology have been enabled by developments in computing. The digitisation of information captured by surveillance technologies creates the potential for preservation of digital footprints of the real-world movements and transactions of individuals.[67] The significance of this is exponential if combined with digital trails captured from use of computers and the internet, as such aggregation could provide very detailed pictures of the online and real-world lives of individuals.

6.48 The ability for information gathered by surveillance technologies to be digitised and stored on computers has greatly expanded the potential usefulness of that information and the potential for that information to be aggregated with other information stored about an individual.[68] Databases multiply the effects of surveillance sensors and make it possible to create new information by combining data in new ways.[69]

6.49 Haggerty and Ericson describe the underlying driver of surveillance as the "desire to bring systems together, to combine practices and technologies and integrate them into a larger whole."[70] A key development is the trend towards networked connectivity and the convergence of various technologies:[71]

> Cameras are only a single feature of a much larger and more sophisticated network. The "digital nervous system" is, or at some point will be, an *integrated* system. Surveillance

65 National Research Council of the National Academies, above n 9, 101.

66 Clive Norris, Jade Moran & Gary Armstrong "Algorithmic Surveillance: The Future of Automated Visual Surveillance" in Clive Norris, Jade Moran and Gary Armstrong (eds) *Surveillance, Closed Circuit Television and Social Control* (Ashgate, Aldershot, 1999) 255, 257-258.

67 Haggerty and Ericson, above n 64, 67-72, discussing "data doubles" and the commodification of the self; Clive Norris and Gary Armstrong *The Maximum Surveillance Society: The Rise of CCTV* (Berg, Oxford, 1999) 221, discussing the "digital persona".

68 See further paras 6.9-6.18 above.

69 Froomkin, above n 64, 1469.

70 Haggerty and Ericson, above n 64, 66.

71 Timothy Zick "Clouds, Cameras and Computers: The First Amendment and Networked Public Places" (2007) 59 Fla L Rev 1, 22.

cameras will be linked to public Web access. Mobile data tags will be linked to surveillance technologies. Personal computing devices will link to the environment, to other devices, to surveillance networks, and to various information clearinghouses on the Web.

6.50 The ultimate convergence issue is the trend towards "ubiquitous" or "pervasive" computing[72] and the "internet of things", in which "the internet does not only link computers and communications terminals, but potentially any of our daily surrounding objects."[73] The possibility under this scenario is a "digitally saturated world" in which surveillance sensors are placed or carried virtually everywhere – for example, in our clothes and money, in our houses (appliances, paint, carpet), and in our cars – and are continuously and routinely gathering and storing information.[74] The internet of things will use wireless technology such as RFID (discussed below) together with sensor technologies and miniaturising technologies such as nanotechnology.[75]

6.51 We have identified two key motivators to the growth of surveillance technologies:

- The commercial advantages in developing and applying technology to gather personal information, including targeting direct marketing to consumers and gleaning information about personal habits and preferences that can direct enhancements in business practice.
- The security imperative that requires the gathering and analysis of personal information to combat crime and the threat of terrorism, and enhance perceptions of public safety.

6.52 Countries such as the United Kingdom and the United States have seen a rapid increase in the level of surveillance of public spaces, in response to fears about terrorism and crime. The routine monitoring and recording of the everyday behaviour of citizens brings into existence large amounts of data that can be scrutinised for suspicious behaviours, either at the time it is created or afterwards.

6.53 But surveillance is not carried out only by government agencies or by business interests. The social context is that surveillance technologies have been "democratised" and are now in the hands of ordinary citizens. This is not necessarily through purchases of spyware, but simply through citizens owning and using legitimate devices such as cellphones containing cameras, and security cameras. Individual surveillance, much of it inadvertent, is expected to exceed official intrusions in scope and detail.[76] This shift creates another contrast between the old surveillance and the new surveillance:[77]

---

72 Also known in Europe as "ambient intelligence"; see the work of the SWAMI (Safeguards in the World of Ambient Intelligence) Consortium, including Michael Friedewald, Elena Vildjiounaite and David Wright (eds) *The Brave New World of Ambient Intelligence: A State-of-the-Art Review* (report of the SWAMI consortium to the European Commission, 2005); 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).

73 European Information Society and Media Commissioner Viviane Reding, quoted in "RFID Chips will Force Changes to Privacy and Electronic Communications Directive" (20 March 2007) www.out-law.com (accessed 21 March 2007).

74 Punie, Delaitre, Maghiros & Wright, above n 72, 6.

75 Australian Law Reform Commission, above n 15, 320.

76 Werbach, above n 63, 2341.

77 Ibid, 2364.

> In short, traditional conceptions of surveillance and privacy are based on small numbers of people obtaining large amounts of information about small numbers of people. Pervasive sensors herald a world in which large numbers of people obtain small amounts of information about equally large numbers of subjects, and that information can be shared and combined easily.

6.54 Surveillance has two faces, with the potential to bring both positive benefits, such as preventing and detecting crime, and negative impacts, such as the curtailing of rights.[78] It is important to note that the new surveillance technologies, just like the old technologies that predated them, can be used entirely appropriately while carrying the potential for inappropriate use or abuse. While surveillance technologies may be used appropriately in the collection of information, the risk of abuse may arise following collection through secondary usage by aggregation or analysis, or through unauthorised disclosure of the information. Surveillance also poses broader ethical and human rights dilemmas, due to its discrimination between groups, "advantaging some and, by the same token, disadvantaging others."[79] This feature of surveillance is known as social sorting. It has been noted that surveillance "that was once reserved for the 'suspect' or 'deviant', has become extended to cover the majority of the population, which can then be sorted, categorised and targeted."[80]

The privacy implications

6.55 To some extent, the new surveillance raises similar privacy concerns to other forms of personal data collection, namely the security of collected data and the potential for misuse and unauthorised disclosure; the use of surveillance data in data matching and data mining; the risk of function creep where information gathered for one purpose is used for another purpose; and the nuisance of targeted advertising.

6.56 However, the new surveillance also exacerbates the privacy concerns associated with traditional surveillance. Surveillance increases a person's visibility, thus detracting from his or her privacy. As one interviewee remarked to a researcher: "When I am on the street I don't wonder whether people are looking at me or not – so how come I was so uneasy in front of that camera?"[81] Concerns have been expressed that the expansion of surveillance may diminish individual autonomy or even personhood, "as individuals no longer have control over, or even knowledge of the situations in which information about them is communicated."[82]

---

78 Nick Taylor "State Surveillance and the Right to Privacy" in Clive Norris and Dean Wilson (eds) *Surveillance, Crime and Social Control* (Ashgate, Aldershot, 2006) 175. See also Surveillance Studies Network, above n 16, 2.

79 Surveillance Studies Network, above n 16, 6.

80 Ibid, 30; see also 8, 30-33. Social sorting is a key theme in the work of David Lyon; see for example "Surveillance as Social Sorting: Computer Codes and Mobile Bodies" in David Lyon (ed) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (Routledge, London, 2003) 13; "Everyday Surveillance: Personal Data and Social Classification" (2002) 5 Information, Communication and Society 242.

81 Quoted in Hille Koskela "Video Surveillance, Gender and the Safety of Public Urban Space: 'Peeping Tom' Goes High Tech?" in Clive Norris and Dean Wilson (eds) *Surveillance, Crime and Social Control* (Ashgate, Aldershot, 2006) 195; see also 204.

82 Norris and Armstrong, above n 67, 223, summarising David Lyon *The Electronic Eye: The Rise of Surveillance Society* (Polity Press, Cambridge, 1994).

6.57 The drive towards integrated or joined-up surveillance raises the risk of "surveillance creep", as multiple uses are found for technologies and as information gathered for one purpose or in one domain leaks through into others.[83] Algorithmic surveillance (the use of software to work on captured images or data and compare them to those in a database)[84] can also intensify the problems of traditional surveillance.[85] A key concern is the use of surveillance information for profiling through data mining. In particular, there are concerns about accuracy,[86] and about the increasing specificity of profiling:[87]

> The threats to privacy are more than just the enhanced ability to track an individual through a set of interactions and activities, although that by itself can be a cause for alarm. It is now possible to group people into smaller and smaller groups based on their preferences, habits and activities. There is nothing that categorically rules out the possibility that in some cases, the size of the group can be made as small as one, thus identifying an individual based on some set of characteristics having to do with the activities of that individual. Furthermore, data used for this purpose may have been gathered for other, completely different purposes.

6.58 The new surveillance also illustrates another privacy concern: the adjustment of privacy expectations as new technologies become ubiquitous. A situation in which society gets used to the gradual erosion of liberty has been compared to the fable of the "boiled frog": the frog fails to jump out of the saucepan as the water gradually heats.[88]

6.59 It can be difficult for citizens to appreciate the privacy implications of routine surveillance and the collection of information that is not of itself discreditable or embarrassing. The laissez faire attitude "if I've got nothing to hide, I've got nothing to worry about" is prevalent, particularly where the surveillance is justified for public interest reasons such as security.[89]

The technologies

6.60 The primary elements of the new surveillance are visual surveillance devices (cameras); wireless sensor networks such as radio frequency identification technology that share information with other machines; and networked devices incorporating location data.[90] We briefly outline the key elements of these technologies below.

83 Surveillance Studies Network, above n 16, 26.

84 Ibid, 20.

85 Stephen Graham and David Wood "Digitizing Surveillance: Categorisation, Space, Inequality" in Clive Norris and Dean Wilson (eds) *Surveillance, Crime and Social Control* (Ashgate, Aldershot, 2006) 543-544.

86 "Learning to Live With Big Brother" (27 September 2007) *The Economist* 60.

87 National Research Council of the National Academies, above n 9, 97. For a description of profiling, see Surveillance Studies Network, above n 16, 20-21.

88 "Learning to live with Big Brother", above n 86, 62. See also Surveillance Studies Network, above n 16, 47.

89 Daniel J Solove *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy* (George Washington University Law School Public Law Research Paper no 289, 2007).

90 Werbach, above n 63, 2324.

Visual surveillance

6.61 There are two striking developments in visual surveillance. The first is the increasing use of closed circuit television (CCTV) cameras in certain countries, and the development of enhancements to CCTV. The second is the increasing capacity of mobile phones to act as surveillance devices.

6.62 Modern surveillance camera systems are no longer "closed circuit" and are increasingly networked digital cameras.[91] However the term "CCTV" is still used to describe surveillance cameras that operate in public spaces. In the United Kingdom, it is estimated that authorities have installed around 4 million security cameras and that the average Londoner is caught on camera some 300 times per day.[92] The pervasiveness of CCTV in the United Kingdom has raised the suggestion that it will become a kind of fifth utility after gas, electricity, water and telecommunications.[93] The Home Office has recently released a *National CCTV Strategy* that makes a number of recommendations about standards, guidelines, registration and regulation in relation to the use of CCTV in the United Kingdom.[94] Many US cities are also implementing CCTV surveillance initiatives.

6.63 It is unclear how many CCTV cameras operate in New Zealand. Numerous businesses operate their own security cameras, as do some schools. In Wellington, there are three City Council street surveillance cameras in the inner city, cameras on some commuter trains,[95] and traffic management cameras.[96] In central Auckland, 49 CCTV cameras were installed several years ago in a joint venture between business group Heart of the City, the police and Auckland City Council, and there are many other cameras in particular shopping and transport precincts.[97] Councils in Lower Hutt, Wanganui, Hastings, Napier and Gisborne also use CCTV for street surveillance.[98]

---

91 Royal Academy of Engineering *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (Royal Academy of Engineering, London, 2007) 34.

92 John Leicester "Europe, US Take UK Lead on Cameras" (10 July 2007) *Washington Post* www.washingtonpost.com (accessed 11 July 2007). While these figures are the best estimate, coverage may not be as extensive as these figures suggest: see Graeme Gerrard, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill and Sarah Douglas *National CCTV Strategy* (United Kingdom Home Office/Association of Chief Police Officers, 2007) 13-15. Nevertheless, use of CCTV in the UK has resulted in a "public space CCTV surveillance infrastructure that is the envy of many police forces around the world": ibid, 28.

93 Stephen Graham "Towards the Fifth Utility? On the Extension and Normalisation of Public CCTV" in C Norris, J Moran and G Armstrong (eds) *Surveillance, Closed Circuit Television and Social Control* (Ashgate Publishing Company, Aldershot, 1999) 89.

94 Gerrard, Parkins, Cunningham, Jones, Hill and Douglas, above n 92.

95 Patrick Crewdson "Sleepwalking into a Surveillance Society" (10 April 2007) *Dominion Post* Wellington A1.

96 CityLink provide online webcams: WatchNET Webcams at www.citylink.co.nz (accessed 26 November 2007).

97 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).

98 Keri Welham "Watching Everything You Do" (10 April 2007) *Dominion Post* Wellington A4.

6.64 There is some debate as to whether CCTV actually reduces crime.[99] There have been instances where CCTV footage has recorded events leading up to high-profile crimes, including the murder of two-year-old James Bulger in Liverpool in 1993, and the London terrorist bomb attacks on 21 July 2005. However, there are questions about the reliability of identification based on CCTV images.[100] There is also debate about whether CCTV improves security, particularly for women.[101]

6.65 As well as the new scale of CCTV coverage in cities in the United Kingdom and the United States, CCTV is notable for new features arising out of technological change and convergence.[102] For example, surveillance cameras can be equipped with loudspeakers allowing operators to bark commands at people who drop litter, act in an aggressive manner or loiter; behaviour-monitoring cameras sound an alarm when an operator spots "suspicious" behaviour; and face-scanning cameras use face-recognition software to match faces in the crowd with faces in the database.[103] London police have installed a system that matches CCTV photographs taken from cameras in shopping centres, parking lots and railway stations with stored images of known criminals.[104] The New Zealand Police are also proposing to use face-recognition software to check for matches against its database of around 800,000 images.[105]

6.66 Future enhancements to CCTV include eavesdropping cameras, lip-reading cameras and X-ray cameras that allow operators to see through people's clothes and look for suspicious items.[106] Experimental work is also being done in the United States to invent a system using biometric information whereby a facial image can be matched to a person's gait, height, weight and other elements so that a computer can identify a person and track that person through a crowd.[107] Next-generation facial recognition software may also allow cameras to gauge a person's thoughts by mapping facial geometry using algorithms.[108] Convergence with radio frequency identification technology (discussed further below) is another possible development, where cameras capture information held on RFID tags embedded in identity cards, clothing, cellphones or other items and potentially any other information linked to a person held on national databases.[109]

---

99 Martin Gill and Angela Spriggs *Assessing the Impact of CCTV* (Home Office Research, Development and Statistics Directorate, London, 2005) 48, 60-61; Mark Schlosberg and Nicole A Ozer *Under the Watchful Eye: The Proliferation of Video Surveillance Systems in California* (American Civil Liberties Union of Northern California, San Francisco, 2007); Adrienne Isnard "Can Surveillance Cameras be Successful in Preventing Crime and Controlling Anti-Social Behaviours?" (Paper presented to the Australian Institute of Criminology, Townsville, August 2001).

100 Ruth Costigan "Identification from CCTV: The Risk of Injustice" [2007] Crim LR 591.

101 See 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) 98; Sheila Brown "What's the Problem, Girls? CCTV and the Gendering of Public Safety" in C Norris, J Moran and G Armstrong (eds) *Surveillance, Closed Circuit Television and Social Control* (Ashgate Publishing Company, Aldershot, 1999) 207, 218; Koskela, above n 81, 195.

102 For a summary of CCTV emerging technologies and techniques, see Gerrard, Parkins, Cunningham, Jones, Hill and Douglas, above n 92, ch 9.

103 Steve Watson "Lip Reading Surveillance Cameras to Stop Terror" (27 April 2007) http://infowars.net (accessed 3 May 2007).

104 Froomkin, above n 64, 1478.

105 "Police Embrace Face Scans" (1 October 2007) www.stuff.co.nz (accessed 1 October 2007).

106 Watson, above n 103.

107 Humphrey Hawksley "Big Brother is Watching us All" (15 September 2007) www.news.bbc.co.uk (accessed 4 October 2007).

108 Zick, above n 71, 41.

109 Schlosberg and Ozer, above n 99.

6.67 Development work is also being done on the mobility of visual surveillance. The United States Defence Department has developed robotic fliers that range from the size of small planes down to the size of birds. Various projects are attempting to produce surveillance tools the size of insects, either by developing robo-bugs or insect-robot hybrids.[110] One hybrid project aims to produce camera-carrying insects whose nerves have grown into their internal silicon chip and whose flight muscles can be remotely controlled.[111]

6.68 The second striking development in visual surveillance is the ubiquity of the camera phone. Cameras are becoming a default feature of mobile phones, and are becoming more capable. The significant feature about camera phones is that they are inherently networked, including the capability not only to take photographs but also to distribute them instantly to other devices or to websites.[112]

6.69 Internet-connected video webcams are also being used as surveillance devices for personal or family security. For example, nannycams are being used to keep an eye on nannies caring for children. In the United States, services such as ParentWatch and Kindercam link to childcare centres allowing parents to observe both their children and caregivers.[113]

6.70 In relation to the surveillance of public places, privacy advocates have enunciated the following concerns:

- the undermining of an ordinary citizen's anonymity while in public,[114] resulting in a dampening of spontaneous behaviour and increasing self-vigilance, with a levelling and sterilising effect on public expressive life;[115]
- the chilling effect where surveillance constrains political action such as lawful protests, and implicates other human rights such as freedom of expression and freedom of association;[116]
- the indiscriminate nature of the surveillance and the inability of citizens to agree to or reject surveillance;
- discriminatory and voyeuristic use of surveillance cameras;[117]
- a fundamental shift in the balance of power between citizen and State;[118] and
- a mistrust of government.

Radio frequency identification (RFID)

6.71 RFID technology has been developed as a mechanism for inventory control to replace barcodes. An RFID system has three parts: a tiny chip on each consumer item (an RFID tag) that stores a unique product identifier; an RFID

110 Rick Weiss "Rise of a Robotic Fly on the Wall" (13 October 2007) *Dominion Post* Wellington E6; "The Fly's a Spy" (3 November 2007) *The Economist* 83.

111 Weiss, above n 110.

112 Werbach, above n 63, 2326. See further paras 6.35-6.38 above.

113 www.parentwatch.com; www.kindercam.com.

114 Surveillance Studies Network, above n 16, 38.

115 Zick, above n 71, 61.

116 Norris and Armstrong, above n 67, 224. See also Solove *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, above n 89, 19.

117 Schlosberg and Ozer, above n 99.

118 Simon G Davies "CCTV: A New Battleground for Privacy" in C Norris, J Moran and G Armstrong (eds) *Surveillance, Closed Circuit Television and Social Control* (Ashgate Publishing Company, Aldershot, 1999) 254.

reader; and a computer system attached to the reader having access to an inventory control database. The information database contains extensive product information, such as the product's contents, origins and manufacturing history.[119]

6.72 RFID technology is "likely to become ubiquitous in the very near future".[120] It is expected to deliver significant cost savings in the supply chain, including reduction of theft and counterfeiting, and benefits in organising and monitoring the supply of goods and services. For example Gillette has experimented with "smart shelves" which record the removal of items to the inventory control system for restocking. There is also the potential for RFID to facilitate exchanges and refunds without keeping paper receipts, and to verify warranty protection.[121] The technology could have major benefits for exports of produce from New Zealand, with the potential for RFID tags to include global positioning system (GPS) capabilities (see further below), and temperature and shock sensors. This will allow exporters to know whether the product has exceeded its optimum temperature and whether it has been dropped.[122]

6.73 Microchips are used overseas as road toll-paying devices, on "contactless" payment cards, passports, work uniforms, luggage, library books and ski-passes.[123] RFID has not yet been introduced in stores in New Zealand, but a consumer protection code of practice has been developed in advance of the possible introduction of RFID tagging of goods.[124] A New Zealand RFID Pathfinder group has been formed to coordinate and support organisations interested in the use of RFIDs.[125] Current uses of RFID technology in New Zealand include:

- office swipe cards;
- the new biometric passport;[126]
- wireless sports-timing technology to plot the times of riders in the Lake Taupo Cycle Challenge;[127] and
- microchipping of dogs.[128]

Legislation has also been passed authorising the making of regulations to provide for the embedding of microchips in social security entitlement cards.[129]

---

119 See further, Australian Law Reform Commission, above n 15, 321-323.

120 Henry B Wolfe "Secondary Usage and Mobile Devices" (Paper for Privacy Commissioner, Privacy and Technology Forum, Wellington, 28 August 2007).

121 Teresa Scassa, Theodore Chiasson, Michael Detubide and Anne Uteck "Consumer Privacy and Radio Frequency Identification Technology" (2005-2006) 37 Ottawa L Rev 220.

122 Ken Lewis "RFID Set to Take Off in NZ as EU Fears Grow" (17 October 2006) www.m-net.nz (accessed 10 September 2007).

123 Todd Lewan "Tracking Technology Chips Away at Privacy" (24 July 2007) *New Zealand Herald* Auckland B3; Marc Langheinrich "RFID and Privacy" (2007) 3 available at http://people.inf.ethz.ch/langhein (accessed 11 December 2007).

124 GS1 New Zealand *EPC/RFID Consumer Protection Code of Practice*; see also www.gs1nz.org.

125 See the website www.rfid-pathfinder.org.nz.

126 Rachael Bowie "Day of the RFIDs" (September 2007) *Consumer* 41. In relation to the biometric passport, see further para 6.94 below.

127 Peter Griffin "All in the Timing for Radio Tag Team" (11 October 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 12 October 2007).

128 Dog Control Act 1996, s 36A; Dog Control (Microchip Transponder) Regulations 2005.

129 The Social Security (Entitlement Cards) Amendment Act 2007, amends the Social Security Act 1964, s 132A(2), to authorise the issuing of regulations on the recommendation of the Minister providing for the embedding of microchips in entitlement cards, subject to adequate consultation under s 132A(4) with the State Services Commission, the Privacy Commissioner and any other State agency considered necessary, to ensure that privacy and personal information are fully protected.

6.74 There is also the potential for RFID technology to be overtly used for tracking people in various contexts or environments, either by individuals carrying an RFID tag or by having a tag implanted.[130] One cited example is the implantation of tags in Alzheimer's patients, so that they can be identified, should they wander from their residence. A corporate provider of surveillance equipment implanted chips in two employees in a well-publicised instance, as a way of restricting access to vaults that held sensitive data.[131] There is also potential for a combination of RFID and wireless fidelity networks (Wi-Fi) to allow real-time tracking of objects or people inside a wireless network, such as a university campus or a hospital.[132] Scientists from University College, London are testing RFID technology to electronically tag passengers at airports to help fight terrorism.[133]

6.75 While the use of RFIDs for inventory control may seem innocuous, privacy concerns arise due to the potential for the RFID data to be aggregated with other information (such as data from loyalty cards or credit cards) "to match product data with personal information in a way that allows for the compilation of highly detailed personal profiles of consumers."[134] There is also concern that if RFIDs become ubiquitous in public places and private homes as well as in private businesses, an infrastructure for surveillance could develop.[135] A European Union Working Party has cautioned:[136]

> The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk through public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviours in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens.

6.76 A specific concern identified in a Resolution on RFID adopted at a conference of International Data Protection and Privacy Commissioners was the potential to use RFIDs "to locate or profile persons possessing tagged objects".[137] For example, knowing that a person's car has passed a certain toll station or that a person's shoes have entered a particular building, allows an observer to infer the location and activity of an observed person.[138]

6.77 A United States consumer survey found that two thirds of respondents indicated that their top concern with RFID technology was "the likelihood that RFIDs

130 For a description of human use of RFID chips, see Surveillance Studies Network, above n 16, 25.

131 Lewan, above n 123.

132 "Wi-fi and RFID Used for Tracking" (25 May 2007) www.news.bbc.co.uk (accessed 30 May 2007).

133 Rebecca Morelle "Air Passengers 'Could be Tagged'" (12 October 2006) www.news.bbc.co.uk (accessed 26 November 2007).

134 Scassa, Chiasson, Detubide and Uteck, above n 121, 246.

135 Electronic Privacy Information Center "Radio Frequency Identification (RFID) Systems" www.epic.org/privacy/rfid (accessed 16 October 2007).

136 Article 29 Data Protection Working Party "Working Document on Data Protection Issues Related to RFID Technology" (19 January 2005) 10107/05/EN WP 105, 2.

137 "Resolution on Radio-Frequency Identification" (Resolution adopted by the International Conference of Data Protection & Privacy Commissioners, November 2003).

138 Langheinrich, above n 123, 9.

would lead to data being shared with third parties, more targeted marketing or the tracking of consumers via their product purchases".[139]

6.78 There are significant security issues with RFIDs such as covert and unauthorised scanning of RFID tags that result in the disclosure of personal information. There are also significant consumer issues such as consumer awareness about whether an item contains an RFID tag, and the remote reading of RFID tags without the person possessing the tagged object being aware or having any opportunity to object.[140]

6.79 A key issue from a privacy law perspective is whether RFID data is "personal information." This will depend on how RFID data is used and integrated with other data and whether this results in the collection, use or disclosure of information about an identifiable individual.

6.80 The tagging of individuals also raises concerns. Critics note that while tagging may begin with vulnerable individuals such as Alzheimer's patients or people with other health conditions, it is conceivable that it will gradually become acceptable for other categories of individuals to be chipped (such as prison inmates, parolees, sex offenders, and illegal immigrants) until a substantial portion of the population is tagged for one reason or another.[141]

Location technologies

6.81 Several developments have created the capability to capture location data. One is the global positioning system (GPS) that utilises satellite signals to ascertain location. GPS chips are now used in vehicle navigation systems and mobile phones. The location data generated from GPS can be enhanced by being integrated into databases and aggregated with other information to create geographic information systems (GIS).[142]

6.82 Cell phones communicate their location to a base station to make or receive calls and so effectively identify the location of the user every few minutes.[143] Vehicle tracking systems are also being developed to manage traffic flow, monitor traffic infringements and administer road payment systems. Some systems, however, have been designed to preserve traveller anonymity.[144]

6.83 Another type of location-based service triangulates position using wireless signals picked up by a laptop, allowing the user to get local weather reports, find nearby restaurants, movie theatres or shops, or share their location with friends. One such service, called Loki, was developed with privacy in mind: the company does not collect user information and subscription is an anonymous process.[145]

---

139 United States Federal Trade Commission *Radio Frequency IDentification: Applications and Implications for Consumers* (workshop report from the staff of the Federal Trade Commission, March 2005) 12.

140 "Resolution on Radio-Frequency Identification", above n 137.

141 Lewan, above n 123.

142 See further, Australian Law Reform Commission, above n 15, 335-337; Werbach, above n 63, 2335. For more detail on tracking technologies, see Katina Michael, Andrew McNamee, MG Michael and Holly Tootwell "Location-based Intelligence – Modeling Behavior in Humans Using GPS" (Paper presented to International Conference of Data Protection and Privacy Commissioners, Montreal, September 2007).

143 Froomkin, above n 64, 1479.

144 Ibid, 1481.

145 Jennifer Cutraro "Privacy Fears Intensified by Tech That Knows Where You Are" (20 October 2006) http://news.nationalgeographic.com (accessed 8 January 2007).

6.84 Some wireless geography-based services now available or still being developed include:[146]

- trip-based car insurance that monitors travel to charge less for coverage on quiet roads and more for heavy traffic;
- using a cell-phone to call the nearest available taxi driver and provide the taxi driver with the location of the cell phone user;
- tracking a jogger's route, distance and speed using phone location-finding technology;
- cell-phone alerts when friends are nearby (social mapping, cited as the next stage in social networking); and
- using a cell-phone to locate the nearest ATM.

6.85 As discussed above, companies such as Google and Microsoft continue to develop location-based services for the internet.[147]

6.86 Moves towards convergence include:[148]

- the GPS capability of mobile phones to automatically tag the location of photographs, creating additional metadata of potential value to photo-sharing websites;[149]
- the incorporation of location-based data into travel-blogs;
- an emerging network known as the "geospatial web" that will utilise computer, cell phone and other mobile devices to enable communication with other nearby users, participation in digital community activities and transmission of advertising from local businesses;[150] and
- the convergence of advanced mapping technology, satellite tracking and wireless communication.[151]

6.87 The concern about GPS-enabled cell phones is the potential to track an individual. There may be legitimate circumstances for tracking. For example, companies may wish to track their employees (subject to workplace privacy issues), and parents might want to check the location of their children. However, there is a concern that anyone could be tracked for less justifiable motives. Another issue is whether law enforcement agencies should be using this type of tracking without authorisation.[152]

146 Jon Van "It's Getting Really Hard to Get Lost" (26 November 2006) *Chicago Tribune* www.chicagotribune.com (accessed 28 November 2006).

147 See further above para 6.39; Werbach, above n 63, 2335-2336.

148 Werbach, above n 63, 2334, 2338.

149 Gordon Haff "Privacy and Geotagging" (25 October 2007) www.cnet.com (accessed 26 October 2007).

150 Cutraro, above n 145.

151 Van, above n 146.

152 Brendan I Koerner "Your Cellphone is a Homing Device" (July/August 2003) *Legal Affairs* www.legalaffairs.org (accessed 27 February 2007).

6.88 GPS technology is giving rise to potential new features such as a service that can tell other contacts where a person is physically located, what communication device they are using and how to reach them. One survey found that while a significant number would like this feature, the majority of those surveyed considered such services an invasion of privacy.[153] Social mapping may give rise to significant security concerns for users, given that it involves divulging location information.[154]

6.89 Froomkin argues that the privacy intrusion of cell phone tracking in real time increases dramatically if location data is archived.[155] There are also concerns about who has access to personal-location information and whether communications systems are secure enough to prevent leaks and misuse of this information. One suggestion is that location information should be continually purged to limit the possibility of it being stolen or mishandled.[156]

TECHNOLOGIES OF THE BODY

6.90 The last set of technological developments that pose major challenges for the protection of privacy is made up of technologies that promise to identify, or unlock the secrets of, the human body itself. Some of these technologies are still very new and are developing rapidly, but in the long term they could be among the developments that have the most profound implications for our sense of privacy. Here we focus on advances in biometrics, genetics and brain science, and the privacy concerns that they give rise to.

6.91 Like technologies of visual and auditory surveillance, technologies of the body have an impact on both informational and local privacy. Our focus here will be on informational privacy, but it is also important to bear in mind that, as we discussed in chapter 3, control over access to the body is a key aspect of local privacy. Some biometric and genetic technologies require the collection of samples in ways that people may find physically intrusive. Even when the physical intrusion is minimal, the very fact that information is being collected about a person's body may feel like an intrusion into control over access to his or her body. Cultural beliefs about the sacred or restricted nature of the body, or of certain parts of the body, will play an important role in determining the degree to which these technologies are experienced as intrusive.[157]

153 Harris Interactive "Survey Shows Privacy Concerns a Major Roadblock for the Adoption of Location-based Services and Presence Technology" (23 February 2007) Press Release www.earthtimes.org (accessed 26 February 2007).

154 Randall Stross "Cellphone as Tracker: X Marks Your Doubts" (19 November 2006) *New York Times* www.nytimes.com (accessed 21 November 2006).

155 Froomkin, above n 64, 1480.

156 Stross, above n 154.

157 For example, in the Employment Court case *OCS Ltd v Service & Food Workers Union Ngā Ringa Tota Inc* (2006) 3 NZELR 558, which concerned the introduction of finger-scanning into a workplace in which most of the employees were Sāmoan, evidence was brought about Sāmoan beliefs about the sacredness of parts of the body: discussed in Paul Roth "Employment Law" [2007] NZ Law Rev 179, 201-202.

Biometric technologies

6.92 Biometric technologies (such as finger and iris scanning, and facial, voice and gait recognition) use biological characteristics to identify individuals.[158] While some of these technologies are new or are still in development, the idea of identifying people by their physical characteristics is a very old one, and the science of biometrics can be traced back to the late-19th century.[159] Modern biometric technologies generally involve taking a sample from a person and converting the sample into digital data that can be stored in a database or an object in the individual's possession. The stored biometric data can be compared to later samples in order to identify the person. So, for example, a company might scan the fingers of its employees when they commence employment and store that information. When the employees start work each day they would have their fingers scanned again, thereby registering that they have "clocked in" for the day. Biometric technologies can be used both to verify that individuals are who they claim to be (verification, or one-to-one matching) and to determine who an unidentified individual is (identification, or one-to-many matching).

6.93 Advocates of increased use of biometric technologies argue that they are a reliable, efficient and easy method of identification. They do not require people to remember passwords or numbers; are based on identifying information that is unique to each individual; can be used for remote electronic transactions (for example, to authenticate a person accessing a secure website via the internet); and in some cases may be easier for people with certain disabilities to use. Technological advances are also making biometric technologies increasingly attractive to both government and business. Because biometric data can be stored on computers, the ability to store and analyse this data has benefited from the advances in computing discussed earlier in this chapter. In addition, emerging biometric technologies make it possible to carry out identification that is automated, performed within seconds, and conducted from a distance, perhaps without the subject's knowledge.

6.94 Biometric technologies are already used in New Zealand by both government and the private sector. New Zealand passports now include a microchip containing a biometric identifier in the form of a digitised image of the passport holder's photograph, making it possible for border control to use facial recognition technology to check people's identities. The Immigration Bill currently before Parliament provides for the use of fingerprints and iris scans as well as photographs.[160]

158 See Malcolm Crompton "Biometrics and Privacy: The End of the World as we Know it or the White Knight of Privacy?" (Paper presented to Biometrics – Security and Authentication, Biometrics Institute Conference, Sydney, 20 March 2002); Marie Shroff (Speech to Biometrics Institute Trans-Tasman Standardisation for Biometrics Conference, Wellington, 1 October 2004); Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy *Biometric-Based Technologies* (2004); Darcie Sherman *Biometric Technology: The Impact on Privacy* (Comparative Research in Law and Political Economy Research Paper Series 5/2005, Osgoode Hall Law School, York University, Toronto, Canada, 2005); National Research Council of the National Academies, above n 9, 106-107; Australian Law Reform Commission, above n 15, 330-332; Royal Academy of Engineering, above n 91, 23-24, 26-27.

159 Valentin Groebner *Who Are You? Identification, Deception, and Surveillance in Early Modern Europe* (transl Mark Kyburz and John Peck, Zone Books, New York, 2007); Michelle Perrot (ed) *A History of Private Life* (transl Albert Goldhammer, vol 4, Belknap Press, Cambridge (Mass), 1990) 469-475.

160 "ePassport Frequently Asked Questions" www.passports.govt.nz (accessed 7 October 2007); Immigration Bill, no 132-1, cls 4 (definition of "biometric information"), 29, 50, 88, 92, 98, 138(1)(e), 207, 254-258. Clause 2(2) provides that some of these clauses may come into force at a later date than the rest of the Bill. The Privacy Commissioner has raised concerns about the provisions in the Bill relating to biometric information: Privacy Commissioner "Submission to the Transport and Industrial Relations Committee on the Immigration Bill 2007" 10-12.

6.95 Biometric technologies can be seen as privacy-enhancing, by providing secure barriers to unauthorised access to personal information. However, a number of risks to privacy and other concerns about these technologies have been identified:

- They may make it easier to monitor people and to link information about an individual, particularly if the same biometric identifier is used in different contexts (becoming, in effect, a unique multi-purpose identifier).
- Some biometric technologies, such as facial recognition, can be used to collect information about individuals and to identify them, without their knowledge or consent. For example, a market research company has patented a system which identifies shoppers and tracks their purchase patterns using facial recognition.[161]
- Because it is based on physical characteristics, biometrics may reveal sensitive information, such as information about a person's health, emotional state, or ethnicity.
- The security of biometric information can be compromised. Although biometric identifiers are unique, there are ways of duplicating them so as to fool electronic detectors, and digitised biometric information can be acquired by hackers. Because biometric identifiers are unique physical characteristics, they cannot be cancelled and reissued in the same way as a password or token if biometric data is stolen.
- Biometric identification is not 100 per cent accurate, and even the best systems will produce some false acceptances and false rejections. This can have serious consequences for an affected individual.

Genetic technology

6.96 Rapid advances in understanding of the human genome and in genetic testing are revealing new information about individuals and creating new challenges for the protection of informational privacy.[162] With the exception of identical twins, every person has a unique genetic sequence, and this has been used for some time to identify individuals (for example, to identify criminal suspects or to determine parentage).[163] The use of DNA testing for identification raises some similar privacy issues to biometric technologies, and indeed can be seen as a form

161 Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, above n 158, 13.

162 See Graeme Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (Cambridge University Press, Cambridge, 2002); 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); articles in "Part II – Balancing Privacy and Security" of David Lazer (ed) *DNA and the Criminal Justice System: The Technology of Justice* (MIT Press, Cambridge (Mass), 2004); Carolyn Doyle and Mirko Bagaric *Privacy Law in Australia* (Federation Press, Annandale (NSW), 2005) 161-168; Matthew Taylor "Human Rights Issues Related to Genetic Information and Privacy" in *A Brave New World: Where Biotechnology and Human Rights Intersect* (Government of Canada, 2005); Jennifer Molina *Genetic Privacy: Issues in Aotearoa/New Zealand* (paper for University of Canterbury interdisciplinary research programme "Constructive Conversations/ Kōrero Whakaaetanga: Biotechnologies, Dialogue and Informed Decision-Making", 2005); "Do Not Ask or Do Not Answer? Genetics, Medicine and Insurance" (23 August 2007) *The Economist* www.economist.com (accessed 7 October 2007).

163 On the use of DNA testing to identify criminal suspects see for example Emily Watt "But How do You Balance Science Against Privacy?" (13 October 2007) *Dominion Post* Wellington A1; Ben Hirschler "DNA's Body of Evidence Challenged" (27 October 2007) *Dominion Post* Wellington B2. The New Zealand Law Commission has discussed the use of DNA testing to verify parenthood in *New Issues in Legal Parenthood* (NZLC R88, Wellington, 2005) ch 5.

of biometrics. However, new concerns are now emerging as a result of the sequencing of the human genome in the 1990s. Continuing research in genetics is unlocking information that most people would consider intensely private, particularly information about predisposition to certain diseases. Moreover, the cost of sequencing entire genomes of individuals is falling quickly, with researchers aiming to get the cost down to US$1000 per person.

6.97 The implications of these developments for privacy are enormously complex, and have been the subject of a detailed two-volume report by the Australian Law Reform Commission and the Australian Health Ethics Committee.[164] In New Zealand, the Human Genome Research Project at the University of Otago, a multidisciplinary project led by the Law Faculty, will be examining genetic privacy in the third year of the project, with a report to be published in 2008.[165]

6.98 One major concern is that the release of information about a person's genetic makeup could lead to discrimination, particularly in the areas of insurance and employment. Another challenge is the fact that, while a person's total genetic sequence is unique, individuals will share important elements of their genetic makeup with relatives. In particular, some genetic disorders are inherited. This means that facts that could be considered private health information of a particular individual also have implications for the health of that person's relatives. It can be argued, therefore, that these relatives also have rights or interests in this information. At the same time, some relatives may claim a "right not to know" information about the likelihood that they will develop a debilitating or fatal disease.[166]

6.99 A key area of disagreement about genetic information is whether it is fundamentally different in nature from other forms of health information. This has implications for whether a separate regulatory regime is necessary for genetic information. Three aspects of genetic information can be seen as distinctive:[167]

- It is ubiquitous; that is, every cell of a person's body (with the exception of sex cells and mature blood cells) contains his or her complete genetic code. As a result, tiny bits of biological material left behind in the course of everyday life can be tested to reveal important personal information.
- It is partially shared with relatives.
- It is predictive, although it usually only indicates possibilities rather than certainties – for example, the fact that a person has a genetic mutation linked to a particular disease does not necessarily mean that he or she will go on to develop that disease.

6.100 These distinctive features of genetic information are cited in favour of "genetic exceptionalism", the view that such information is "uniquely powerful and [poses] special threats to privacy and discrimination that mandate dedicated and higher levels of legal protection".[168] By contrast, "genetic inclusivists" argue that

164 *Essentially Yours: The Protection of Human Genetic Information in Australia*, above n 162.

165 See www.otago.ac.nz/law/genome (accessed 7 October 2007). The Human Genome Research Project has already discussed privacy and confidentiality issues in relation to genetic testing of minors in *Genes, Society and the Future* (vol 2, Human Genome Research Project, Dunedin, 2007) 426-436.

166 *Essentially Yours: The Protection of Human Genetic Information in Australia*, above n 162, 133-134.

167 Ibid, 132-137.

168 Ibid, 137.

genetic information is not different from other types of health information, and that no special regime or protections are needed. They point out that other types of information, such as information about lifestyle or non-genetic test results, can also be predictive, and can likewise lead to discrimination.[169]

6.101 Another difficult legal issue is whether genetic samples constitute "information" for the purposes of privacy protection. Advances in genetics are increasingly blurring the distinction between bodily tissue and information. The Australian Law Reform Commission and Australian Health Ethics Committee considered this question in relation to the Privacy Act 1988 (Cth), and recommended that genetic samples should be included in the definitions of "personal information" and "record" in the Act. This recommendation was rejected by the Australian Government.[170]

Brain scanning

6.102 Psychological testing has long been of concern to privacy advocates,[171] and recent developments in brain science are leading to renewed fears of intrusions into "mental" or "dispositional" privacy. The realm of a person's private thoughts can be considered the ultimate refuge from the outside world, but advances in the understanding of brain functioning may threaten this privacy. Technologies that scan the brain and show how regions respond to stimuli such as words or images may be used to reveal whether people are lying, whether they are experiencing hostile or racist thoughts or feelings, or which commercial products they respond to most positively, for example. Such developments are still at an early stage, but may have very significant impacts on privacy in future.[172]

PRIVACY-ENHANCING TECHNOLOGIES

6.103 So far in this chapter we have discussed the ways in which new and emerging technologies may be used to intrude on privacy. However, technology can also be used to enhance privacy, and a variety of technological solutions have been proposed to some of the concerns identified above.[173] It is important that proposals for law reform take into account the positive role of privacy-enhancing technologies (PETs), rather than simply focusing on the negative impacts of technology on privacy. In this section we will not catalogue the many different kinds of PETs, but will provide some illustrative examples.

169 This debate is summarised in ibid, 137-140.

170 Ibid, ch 8; Australian Law Reform Commission, above n 15, 333-334.

171 See Alan F Westin *Privacy and Freedom* (Atheneum, New York, 1967) chs 6, 9, 10.

172 Henry T Greely "Neuroethics: The Neuroscience Revolution, Ethics, and the Law" (Lecture at the Markkula Center for Applied Ethics, Santa Clara University, California, 20 April 2004); *Connecting Brains and Society: The Present and Future of Brain Science – What is Possible, What is Desirable?* (King Baudouin Foundation/Rathenau Institute, Brussels/The Hague, 2004) 167-173; Barbara Nicolas *Neuroethics: A Literature Review Prepared for Toi te Taiao: The Bioethics Council* (2006) 17-18; Steven PR Rose *Future Directions in Neuroscience: A Twenty Year Timescale* (briefing prepared for the New Zealand Navigator Network, 2007) especially 26-27; Steven Rose "We are Moving Ever Closer to the Era of Mind Control" (5 February 2006) *Observer* http://observer.guardian.co.uk (accessed 25 October 2007); Francine Russo "Who Should Read Your Mind?" and Alice Park "Marketing to Your Mind" (19 January 2007) *Time* www.time.com (accessed 7 February 2007).

173 For some general discussions of privacy-enhancing technologies, and examples of particular technologies, see Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy *Inventory of Privacy-Enhancing Technologies (PETs)* (2002); Bennett and Raab, above n 2, ch 7; International Telecommunication Union *Digital.Life: ITU Internet Report 2006* (Geneva, 2006) 102-120; Australian Law Reform Commission, above n 15, 312-315, 346-349; Royal Academy of Engineering, above n 91, 25-28, 37-43; National Research Council of the National Academies, above n 9, 107-116; George Duncan "Privacy by Design" (31 August 2007) *Science* 1178-1179.

6.104 PETs should be distinguished from data security technologies, which will not be discussed here. Data security technologies protect information from unauthorised access by third parties, and are necessary but not sufficient for the protection of privacy. It is possible to keep personal data secure when, from a privacy perspective, it should never have been collected or retained in the first place. PETs, by contrast, seek to limit the collection of personal information or to give greater control over that information to the person concerned.[174]

6.105 Broadly speaking, PETs can be divided into those that individuals can choose to employ to protect their own privacy, and those that are built in to technologies or systems at the design stage.

PETs for use by individuals

6.106 Most of the PETs that allow users to take steps to safeguard their own privacy are related to the internet. They include:[175]

- Encryption of information so that it cannot be accessed without the authorisation of the person to whom the information relates (this is arguably a security rather than a privacy protection, however).
- Tools that allow users to maintain complete anonymity while using the internet, or that allow them to adopt pseudonymous online identities. An online pseudonym is an identity issued by a trusted third party, who retains information about the person behind the pseudonym. The owner of the pseudonym is thus able to interact with others on the internet without his or her offline identity being known, and can also adopt multiple online identities in different contexts. If necessary, however, these online and offline identities can be reconnected for law enforcement or other purposes.
- Instruments that block or filter "cookies" and other forms of internet monitoring.
- Technologies that allow users to make informed choices about their internet browsing based on their personal privacy preferences. The best known of these tools is the Platform for Privacy Preferences (P3P), which allows websites to create machine-readable versions of their privacy policies. This in turn makes it possible for users whose browsers are equipped with P3P readers to have their specified privacy preferences automatically compared to the website's privacy policy. Users are notified if the website policy does not match their preferences.

Privacy by design

6.107 It is clearly desirable to design systems in such a way as to minimise their intrusiveness into privacy. This involves clarifying the purpose of the system and designing it so that the smallest possible amount of personal information is stored for the shortest possible time; and carrying out an analysis of potential risks to privacy and strategies to minimise them.[176] Privacy Impact Assessments

174 Bennett and Raab, above n 2, 180; International Telecommunication Union, above n 173, 104. Most PETs protect informational rather than local privacy.

175 Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy *Inventory of Privacy-Enhancing Technologies (PETs)*, above n 173, 17-22; Bennett and Raab, above n 2, 190-197; International Telecommunication Union, above n 173, 102-105.

176 Royal Academy of Engineering, above n 91, 25.

(PIAs) carried out at an early stage in the design of systems can play an important role in identifying privacy risks and suggesting ways of achieving the same objectives by less privacy-intrusive means.[177]

6.108 Online authentication and identification provide examples of ways in which privacy can be designed into systems. It is not always necessary to identify someone to determine whether or not he or she is allowed to engage in a particular activity. For example, it might only be necessary to establish that the person is above a certain age threshold.[178] Nevertheless, there will be many contexts in which it will be necessary to establish the identity of a person seeking to engage in online transactions. This is generally a three-stage process:[179]

- *Verification* involves establishing an identity by such means as choosing a user name and password, or verifying an individual's identity in person.
- *Authentication* involves proving that people are who they say they are by presenting some form of credential: something they have (such as a token), something they know (such as a password), or something they "are" (such as a fingerprint or other biometric indicator).
- *Revocation* involves cancelling an identity when it is no longer required, such as when a person has died or transferred his or her account to another company. Revocation helps to prevent identity theft.

6.109 In New Zealand, innovative work on authentication is being undertaken as part of the e-government programme coordinated by the State Services Commission.[180] A great deal of government information and some personal information on public registers is already available over the internet. However, delivery of some government services online requires ensuring that they are going to the right person. This, in turn, means that the identity of people seeking to access those services must be authenticated online.

6.110 Protection of privacy is one of six policy principles for online authentication in e-government transactions, which were approved by Cabinet in 2002. Privacy has been considered at each stage of the process (concept, design, building and implementation), and multiple PIAs are being carried out at different stages. The "designing in" of privacy protection is intended to avoid risks such as unauthorised information matching, loss of control over personal information, or the creation of a national identity card or other unique multi-purpose identifier. The system will allow for a common means of verifying identity and

177 For more on Privacy Impact Assessments see Office of the Privacy Commissioner *Privacy Impact Assessment Handbook* (Wellington, 2007); Information Commissioner's Office (United Kingdom) *PIA Handbook* (2007) available at www.ico.gov.uk (accessed 18 December 2007); Linden Consulting *Privacy Impact Assessments: International Study of their Application and Effects* (report prepared for the Information Commissioner's Office, United Kingdom, October 2007), especially Appendix F – "Jurisdictional Report for New Zealand".

178 Royal Academy of Engineering, above n 91, 37-38; National Research Council of the National Academies, above n 9, 115.

179 International Telecommunication Union, above n 173, 114; Australian Law Reform Commission, above n 15, 314-315.

180 Laurence Millar "Connected Government: The New Zealand Story" in Willi Kaczorowski (ed) *Connected Government: Thought Leaders. Essays from Innovators* (Premium Publishing, London, 2004) 24; Liberty Alliance Project "Case Study: New Zealand Sets the Pace for SAML 2.0 Deployments" www.projectliberty.org (accessed 9 October 2007); www.e.govt.nz/services/authentication (accessed 9 October 2007); presentations by State Services Commission to Law Commission, 1 May 2007 and 14 September 2007.

a single log-on for each individual across all online government services.[181] Privacy protections include ensuring that log-on is separated from authorisation of access; that only the minimum possible personal information required is stored for identity verification purposes; that only the identity data actually required by a particular agency is transmitted to that agency, and only with the active consent of the person concerned; and that no common unique identifier is generated in the authentication process.

6.111 Design solutions are also being sought for some of the privacy concerns with specific technologies discussed in this chapter:

- Various privacy-protection techniques have been proposed for video surveillance, with the aim of preserving the usefulness of video footage while also preserving the privacy of innocent people whose images happen to be captured by video cameras. Researchers are working on techniques for de-identifying faces and other privacy-sensitive details such as car licence plates in video footage. In some of these techniques, the scrambling of parts of the image can be reversed by authorised users who have a decryption key.[182] Significant technical problems remain, however, and "existing techniques are too expensive and slow to be used in general video surveillance".[183]
- A variety of PETs have been developed for use with RFID technologies. These include deactivating RFID tags on products once they have been purchased; encrypting data on RFID tags; and "clipping" antennae on RFID tags to reduce the range at which they can be read.[184] Another approach is designing RFID systems so that there is no link between the information stored on the RFID tag and an individual's personal information.
- Biometric encryption uses a biometric as a key to encrypt and decrypt a password, personal identification number or alphanumeric string, which can then be used for access and identification purposes. Unlike existing biometric technologies, no biometric sample or template would be retained. It has been claimed that biometric encryption would eliminate the privacy concerns with biometric technologies. However, there are significant technological challenges to the creation of workable biometric encryption, and the technique is not yet operational.[185]

---

181 Public consultation documents have been released in relation to the proposed online identity verification system: see www.dia.govt.nz/idconsult. See also Tom Pullar-Strecker "Government, Businesses May Share Online ID System" (29 October 2007) *Dominion Post* Wellington www.stuff.co.nz (accessed 28 November 2007); "Civil Liberties Fears Online ID System" (12 November 2007) *Dominion Post* Wellington www.stuff.co.nz (accessed 12 November 2007); Claire McEntee "Profiling Danger in Identity System" (10 December 2007) *Dominion Post* Wellington www.stuff.co.nz (accessed 11 December 2007).

182 Frederic Dufaux and Touradj Ebrahimi "Privacy-Protection Technology for Video Surveillance" http://spie.org (accessed 12 October 2007); see also Royal Academy of Engineering, above n 91, 42 for a suggestion of automated surveillance systems that would only alert a human operator when suspicious activity is detected.

183 Duncan, above n 173, 1179.

184 Maarten van de Voort and Andreas Ligtvoet *Towards an RFID Policy for Europe: Workshop Report* (European Commission, Directorate General Information Society and Media, 2007) 20-21.

185 Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy *Biometric-Based Technologies*, above n 158, 64-66; Ann Cavoukian and Alex Stoianov *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (Information and Privacy Commission (Ontario), Toronto, 2007); "Interview with Dr Ann Cavoukian" (June 2007) www.nymity.com (accessed 5 October 2007).

It is important to note that work on some of these PETs is still continuing, and it is by no means clear that they will provide workable solutions to privacy concerns.

PETs and law reform

6.112 Bennett and Raab identify three roles for PETs as instruments of privacy policy:[186]

- They can complement other regulatory approaches, being seen as an important part of the "toolbox" but insufficient on their own to protect privacy adequately.
- They can be used as conditions or standards, which may be specified in legislation, regulations or codes of practice. That is, a particular product or service might be required to incorporate specified PETs, providing specified levels of protection.
- They can be presented as alternatives to regulation. This approach has been advocated in the United States as a way of avoiding stricter privacy laws, and has been criticised by privacy advocates.

Both the European Commission and the Australian Law Reform Commission have recently supported the view that PETs can play an important role in complementing, but not replacing, legislative and regulatory frameworks for protecting privacy.[187]

6.113 As well as considering how the privacy-intrusive effects of technology can be restricted by the law, law reform should address the ways in which law and policy might be able to protect privacy by promoting the use of PETs. There are many possible roles for law and government policy in promoting PETs, including:[188]

- Promoting and supporting research into and development of PETs.
- Adopting PET-friendly policies within government departments and agencies. This can include using PETs in the government's own information systems and other technologies that may have implications for privacy, ensuring that privacy is designed in to new systems, and carrying out privacy impact assessments of systems during and after development.
- Requiring the incorporation and use of PETs in the provision of particular products and services.
- Intervening directly in the design of systems by private companies. While this is unlikely to happen often, one significant example is the European Union's successful attempt to get Microsoft to modify its Passport system (discussed further in chapter 7).

186 Bennett and Raab, above n 2, 198-202.

187 Commission of the European Communities *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)* (2 May 2007) COM(2007) 228, 4; Australian Law Reform Commission, above n 15, 348.

188 Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy *Inventory of Privacy-Enhancing Technologies (PETs)*, above n 173, 25-26; Bennett and Raab, above n 2, 198-199; Commission of the European Communities, above n 187, 5-10; Ralf Bendrath *Privacy Self-Regulation and the Changing Role of the State: From Public Law to Social and Technical Mechanisms of Governance* (TranState Working Paper no 59, Transformations of the State Collaborative Research Center, University of Bremen, Germany, 2007) 29-30.

- Removing legal and other obstacles to the use of PETs by consumers, so long as these PETs do not protect privacy at the expense of other public interests (some restrictions on the use of encryption and anonymisation may be needed for security and law enforcement purposes, for example).
- Raising consumer awareness of PETs through provision of information and education.
- Facilitating informed choice by consumers through the development of privacy standards for technologies and associated certification programmes such as privacy seals.

CONCLUSION

6.114 The technologies that we have discussed in this chapter can play enormously beneficial roles in our individual lives, and in the life of our society. The ever-increasing capacity of computers allows us to process vast amounts of information in a short space of time, making possible major advances in business, medicine, science and other fields. The internet is facilitating the free flow of information, and creating new spaces for dialogue and participation. RFID chips can be invaluable to businesses when used to track products from point of manufacture to point of sale. Our growing knowledge of human genetics and brain functioning may help to find cures for previously incurable diseases. The challenge, then, is to find ways of gaining the benefits of these technologies while minimising or eliminating the risks to privacy.

6.115 This chapter has shown that there are indeed many risks to privacy from current technologies and technologies that are still under development. New risks from current technologies may also emerge in future as a result of "function creep": the discovery of new uses for existing technologies or data. In addition to the threat that technologies may pose individually, digitisation, networking and convergence of technologies increasingly mean that they work as part of integrated systems. These systems may be more powerful than the sum of their parts, and may have unforeseen consequences. It has been suggested that the integration of technologies of visual surveillance, facial recognition, location and data collection could "raise the prospect of a society in which everyone can be automatically tracked at all times".[189]

6.116 There is also a danger that technological fatalism can be a self-fulfilling prophecy, however. As we suggested at the start of this chapter, technology is not a completely autonomous force. Technologies are human creations, and while we cannot entirely predict their social consequences, we can shape them to a significant extent. The law has an important role to play in this process, even though there is often a lag between the emergence of new technologies and legal responses to them.

6.117 Technological change may have a number of implications for the law, which law reform may need to address.[190] We have already referred to the creation of new risks. Sometimes the enforcement of existing laws and regulations will be adequate to deal with these risks, but in other cases the laws may need to be modified or replaced, or an additional law may be needed to cover the new technology. Other possible implications of technological change also appear relevant to privacy law:

189 National Research Council of the National Academies, above n 9, 106-107.

190 For a general discussion of the law and technological change, see Lyria Bennett Moses "Adapting the Law to Technological Change: A Comparison of Common Law and Legislation" (2003) 26 UNSWLJ 394.

- New technologies may call into question the meaning of existing categories, possibly requiring changes to legislative definitions. In the case of privacy law, the meaning of terms such as "personal information", "news medium" and "publicly available publication" may need to be reconsidered in the age of the internet.
- New technologies may create new difficulties for enforcement of existing laws, as with the questions of jurisdiction and liability in relation to breach of privacy on the internet.
- New technologies may lead to changes in social attitudes, with the result that the law may get out of step with prevailing views in society. In chapter 5 we explored the possibility that young people growing up in a networked world may have different attitudes to privacy from those of previous generations, although even if this is true the implications for the law will take some time to become clear.

6.118 In the later stages of this Review we will consider specific implications of technological change for particular areas of privacy law. We have discussed the digitisation and online availability of public registers, and what this means for privacy, in our *Public Registers* issues paper. The effect of the digital data and networking revolutions on privacy will also be significant issues in stages 3 and 4 of the Review. Another topic for further exploration in those stages is surveillance, following on from our preliminary discussion in chapter 8 of this study paper. Any legal framework for surveillance must take account of the capabilities of the new technologies of visual surveillance, location and biometric identification discussed above.

6.119 Advances in genetics will need to be considered as part of the changing context for health information privacy, a topic we discuss in a preliminary way in chapter 8. However, given the comprehensive report of the Australian Law Reform Commission and Australian Health Ethics Committee, and the ongoing work of Otago University's Human Genome Research Project on this complex topic, it is unlikely that we will examine genetic privacy in detail.

6.120 In stages 3 and 4 we will also need to consider ways in which the legal framework might be able to support technological solutions to privacy problems through the development and use of privacy-enhancing technologies. New Zealand may not be a leading developer of new hardware or software, but our relatively small size may assist in finding innovative ways of protecting privacy in the design of systems, as the example of the e-government programme suggests. For all the undoubted risks to privacy posed by technology, encouraging the incorporation of privacy at the design stage may provide some of the solutions.

Chapter 7:

The International Dimension

7.1 In the preceding chapter we examined the significance of technological developments to privacy. Of particular contextual importance to the discussion in this chapter is the surge in trans-border flows of information that technological innovation has facilitated. Increased connectivity between computers has encouraged extensive transfers of information internationally. The internet has supplied numerous pathways for moving information swiftly around the globe. As one commentator has observed:[1]

> Almost all business processes have become international. Consumer services are supplied out of India, accounts payable out of Costa Ric[a], software development is conducted in the Ukraine, and clinical trials are conducted in as many as twenty countries all at the same time. One global team meeting might require twenty professionals to all look at the same data sets originating from servers in twenty different countries. Industries as diverse as pharmaceuticals, automotive, software development and cosmetics all rely on global teaming and global sourcing. These business processes require massive flows of data across international borders in order to work.

7.2 As a result, information about individual New Zealanders (including their consumption patterns) might be stored and used in jurisdictions beyond New Zealand. Much of this information is of use to commercial operations and to non-governmental organisations. Many types of information processing are now "outsourced" to countries that may not have legal frameworks in place for the protection of privacy.[2]

7.3 Nation-states also have an interest in monitoring the transnational movement of information. Arguably, anxieties concerning terrorism in the early 21st century and the surveillance and control of movements of people

1 Testimony of Martin E Abrahams, Executive Director, Center for Information Policy Leadership, Hunton and Williams LLP, to Hearing on Federal Trade Commission Reauthorization, United States Senate Committee on Commerce, Science and Transportation (Subcommittee on Interstate Commerce, Trade and Tourism) (12 September 2007) 5.

2 Mo Taherzadeh "Privacy and Outsourcing: Evolving Concerns" (7 September 2007) www.mondaq.com (accessed 10 September 2007). For an example of outsourcing of processing of medical information, see Clair Weaver "Aussie Patient Records Outsourced to Philippines" (15 April 2007) www.news.com.au (accessed 17 April 2007).

(including border control and immigration) have accentuated the interest in securing intelligence from flows of data, as well as exchanging information between governments.[3]

7.4 For these reasons, the international legal dimension of privacy is one of increasing importance. As Charles Raab and Colin Bennett have pointed out, "much of the domestic policy activity … has arisen in response to initiatives at the transnational level".[4] For a small jurisdiction such as New Zealand, the international dimension of privacy is unavoidable, not least because of the relevance of international trade to New Zealand and the consequent need to align New Zealand's approaches with those of the other countries it trades with.

7.5 The international privacy instruments that are most relevant to New Zealand are those of the United Nations, the Organisation for Economic Cooperation and Development (OECD) (which comprises some thirty of the globe's most affluent nations) and certain regional arrangements, particularly the Asia-Pacific Economic Cooperation (APEC) grouping and the European Union. In this chapter we summarise these key frameworks with a view to noting issues of relevance to later stages in the Law Commission's Review, and also touch on the development of international privacy standards and the implications of international trade rules. In addition, the chapter discusses the difficult question of legal enforcement in the context of trans-border information flows. Importantly, however, this chapter can only be illustrative and non-exhaustive in view of the relatively complex and dynamic nature of the international regimes regarding privacy and data protection in the 21st century. Other authors have addressed these questions in much greater detail.[5]

3 In this chapter, we do not intend to address this significant area in any detail but it remains an important part of the international context. See Alex Conte *Counter-Terrorism and Human Rights in New Zealand* (New Zealand Law Foundation, Wellington, 2007) especially ch 17; David Dyzenhaus *The Constitution of Law: Legality in a Time of Emergency* (Cambridge University Press, Cambridge, 2006); Andrew Horrell *On Global Order: Power, Values, and the Constitution of International Society* (Oxford University Press, Oxford, 2007); John E Smith *New Zealand's Anti-Terrorism Campaign: Balancing Civil Liberties, National Security, and International Responsibilities* (Ian Axford [New Zealand] Fellowship in Public Policy report, December 2003). Also relevant is the Supreme Court of Canada's decision in *Charkaoui v Canada (Citizenship and Immigration)* [2007] SCC 9, which is briefly discussed in Mark Hickford *A Conceptual Approach to Privacy* (NZLC MP 19, Wellington, 2007).

4 Colin J Bennett and Charles Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge, Massachusetts, 2006) 83.

5 For more detailed discussion of these topics see, for example, L Bygrave "Privacy Protection in a Global Context – A Comparative Overview" (2004) 47 Scandinavian Studies in Law 319; Bennett and Raab, above n 4, ch 4.

THE HUMAN RIGHTS ARENA

7.6 Privacy has been expressed as a human right.[6] Article 12 of the Universal Declaration of Human Rights states that:

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

7.7 The International Covenant on Civil and Political Rights (ICCPR) was ratified by New Zealand in 1978, although the Covenant has not been formally incorporated as a whole into New Zealand's municipal law. Unlike the Universal Declaration of Human Rights, the ICCPR provides mechanisms for complaints of non-compliance with the Covenant to be laid before the United Nations Human Rights Committee. New Zealand is a signatory to the Optional Protocol to the ICCPR, which provides the Human Rights Committee with competence to hear such complaints.

7.8 Article 17 of the ICCPR provides that:

> 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.

Similar provisions are contained in Article 16 of the Convention on the Rights of the Child, which has also been ratified by New Zealand.

7.9 While many of the rights in the ICCPR find expression in the New Zealand Bill of Rights Act 1990, Article 17 has not been incorporated directly into that statute. According to *A Bill of Rights for New Zealand: A White Paper* published in 1985:[7]

> The Bill (like the Canadian Charter) gives no general guarantee of privacy. 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.

7.10 The protection afforded to "privacy" under Article 17 is presumably more comprehensive than that enjoyed by one's "honour and reputation", as no individual is to be subjected to either "arbitrary or unlawful interference with his privacy, family, home or correspondence" whereas the prohibition applies only to "unlawful attacks" on one's "honour and reputation".

6 Katrine Evans, formerly of Victoria University of Wellington and now Assistant Privacy Commissioner – Legal at the Office of the Privacy Commissioner in New Zealand, is currently preparing a useful text on privacy law in New Zealand, which discusses, amongst other things, the human rights dimension of privacy in the international context.

7 Minister of Justice *A Bill of Rights for New Zealand: A White Paper* (Department of Justice, Wellington, 1985) 103-104, para 10.144. For a critique of the non-inclusion of a right to privacy in the New Zealand Bill of Rights Act, see 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).

7.11 What is entailed by "privacy" pursuant to Article 17, however, is not at all clear. As with the concept of privacy in municipal law, the appearance of privacy in Article 17 has occasioned some reference to the uncertainty and indeterminacy of the term "privacy" itself.[8] It has been noted that the meaning of privacy under Article 17 has "not yet been thoroughly defined in either the General Comment or the case law".[9] Indeed, a dissenting opinion in *Coeriel and Aurik v The Netherlands* (453/91) has expressed the view that:[10]

> The Committee itself has not really clarified the notion of privacy … in its General Comment on article 17 where it actually refrains from defining that notion. In its General Comment the Committee attempts to define all the other terms used in article 17 such as "family", "home", "unlawful" and "arbitrary". It further refers to the protection of personal "honour" and "reputation" also mentioned in article 17, but it leaves open the definition of the main right enshrined in that article, [that is,] the right to "privacy".

7.12 In an important text on the ICCPR, Manfred Nowak has suggested that in construing the meaning of "privacy" under Article 17, recourse might be had to the holdings of the "Strasbourg organs" of the European Union (such as the European Court of Human Rights) in spite of the slight divergence in language.[11] Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) states:

> *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 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.

7.13 In Article 10 of the ECHR, freedom of expression is protected:

> 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

8 Sarah Joseph, Jenny Schultz and Melissa Castan (eds) *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary* (2 ed, Oxford University Press, Oxford, 2004) para 16.02.

9 Ibid, 477.

10 Ibid. The General Comment referred to is Human Rights Committee "General Comment No 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17)" (8 April 1988).

11 Manfred Nowak *UN Covenant on Civil and Political Rights: CCPR Commentary* (2 ed, N P Engel, Kehl am Rhein, 2005) 385.

or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

7.14 Article 8 has generated its own sophisticated jurisprudence, which can only be dealt with very briefly and non-exhaustively for our purposes. The range of cases to date would indicate that the phraseology favoured by Article 8 – the reference to "respect for his private and family life, his home and his correspondence" – has permitted a broad and rather fluid approach. Indeed, in *PG and JH v United Kingdom*, the European Court of Human Rights has stated that "private life" in Article 8 "is a broad term not susceptible to exhaustive definition".[12]

7.15 In spite of Nowak's perspective on the comparison between Article 17 of the ICCPR and Article 8 of the European Convention, there is a persuasive view that "privacy" referred to in Article 17 of the ICCPR is not synonymous with "private … life" in Article 8 of the European Convention.[13] Based upon the present case law, one could suggest that the notion of a "private life" in Article 8 is capable of a much broader interpretation than the term "privacy" might otherwise attract.[14] Thus, Article 8 has been treated as contemplating the protection of concepts as broad as a "right to personal development, and the right to establish and develop relationships with other human beings and the outside world".[15] The variety of fact situations emerging has led to an incremental case-by-case approach, but the breadth of the scope of Article 8 continues to be worthy of particular note. It has been held that gender identification, name and sexual orientation, as well as sexual life, are caught within the meaning of Article 8.[16] Furthermore, the guarantee within Article 8 has been interpreted as embracing interests as broad as the rights to live as a gypsy,[17] to be free from severe environmental pollution,[18] to have one's post-operative gender recognised,[19] and to be protected from sexual and physical assault.[20] Other cases have considered issues relating to the refusal to award custody of a child to the applicant because of his homosexuality,[21] the enforcement of legislation

12 *PG and JH v United Kingdom* 44787/98 [2001] Eur Court HR 550 (25 September 2001); [2002] Crim LR 308, para 56. Other cases where the phrase "privacy is a broad term not susceptible to exhaustive definition" has been used include *Peck v United Kingdom* (2003) 36 EHRR 41, para 57; *Niemietz v Germany* (1992) 16 EHRR 97, para 29 and *Pretty v United Kingdom* (2002) 35 EHRR 1, para 61.

13 We are indebted to Nicole Moreham of Victoria University of Wellington for contributing this observation.

14 Depending, of course, on one's underlying conceptual approach to "privacy" in the first instance.

15 *Pretty v United Kingdom*, above n 12, 36, referring to *Burghartz v Switzerland* (1994) 18 EHRR 101, para 47 and *Friedl v Austria* (1996) 21 EHRR 83, para 45. Also refer to *Peck v The United Kingdom*, above n 12; (2003) 36 EHRR 41; 44647/98 [2003] Eur Court HR 44 (28 September 2003) para 57; *Niemietz v Germany*, above n 12; and *Halford v the United Kingdom* 20605/92 (1997) 24 EHRR 523; [1997] Eur Court HR 32 (25 June 1997); [1998] Crim LR 753.

16 For instance, *B v France* (1993) 16 EHRR 1, para 63; *Burghartz v Switzerland*, above n 15, para 24; *Dudgeon v United Kingdom* (1982) 4 EHRR 149, para 41; *Laskey, Jaggard and Brown v United Kingdom* (1997) 24 EHRR 39, para 36.

17 Refer to *Connors v United Kingdom* (2005) 40 EHRR 9; and *Chapman v United Kingdom* (2001) 33 EHRR 18.

18 See for example, *Guerra and others v Italy* (1998) 26 EHRR 357 and *Taskin v Turkey* (2006) 42 EHRR 50.

19 Illustratively, *I v United Kingdom* (2003) 36 EHRR 53; *Goodwin v United Kingdom* (2002) 35 EHRR 18; and *B v France*, above n 16.

20 See *X and Y v Netherlands* (1985) 8 EHRR 235; *MC v Bulgaria* (2005) 40 EHRR 20; and *YF v Turkey* (2004) 39 EHRR 34.

21 *Salgueiro Da Silva Mouta v Portugal* [2001] 1 FCR 653; (2001) 31 EHRR 47.

prohibiting homosexual acts committed in private between consenting males,[22] and access by individuals to information about themselves.[23] A survey of the judicial findings indicates that the European Court has also found interferences with the notion of the "right to respect for his private life" to have occurred in instances such as the following:

- The retention of fingerprints and DNA samples of suspects even when no guilt had been established and when the investigation had been discontinued.[24]
- The use of medical reports in court proceedings concerning the applicant without his consent or without the intervention of a medical expert.[25]

7.16 The right engaged under Article 8 is therefore extremely broad and, in particular, provides extensive protection for the autonomy aspect[26] of the "privacy" interest.

7.17 Importantly, for the purposes of privacy law, Article 10 guarantees the right to receive and to impart information although there is no express entitlement to access information. In *Leander v Sweden* it was held that Article 10, in providing for a right to "receive information" without interference by government, signifies a right that is limited to receiving information "that others wish or may be willing to impart".[27] Interestingly, however, the European Court of Human Rights has suggested that there may be a constrained right of access to information via Article 8, where the information is relevant to the enjoyment of the right to respect for private and family life.[28]

7.18 In *Leander*, the European Court of Human Rights stated that:[29]

> The Court observes that the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart to him. Article 10 (art. 10) does not, in circumstances such as those of the present case, confer on the individual a right of access to a register containing information on his personal position, nor does it embody an obligation on the Government to impart such information to the individual.

7.19 While the European Convention exerts no direct legal effect on New Zealand law, it does influence the jurisprudence of the United Kingdom via the Human Rights Act 1998, which in turn provides a corpus of judicial experience in the balancing of human rights concerns, including the relationship between privacy and freedom of expression.[30] We have already observed that this interface is one of the critical issues confronting any law reform analysis of privacy, and we will return to the issue in chapter 8.

---

22 *Dudgeon v The United Kingdom*, above n 16.

23 Refer to *Gaskin v United Kingdom* (1989) 12 EHRR 36 and *MG v United Kingdom* (2003) 36 EHRR 3 and see the brief discussion below in relation to *Leander v Sweden* Series A, no 116, 29, para 74 (1987).

24 *S and Marper v United Kingdom* 30562/04 and 30566/04 [2007] Eur Court HR (16 January 2007).

25 *Le Lann v France* 7508/02 [2006] Eur Court HR (10 October 2006).

26 "Though no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees": *Pretty v United Kingdom*, above n 12, 36.

27 *Leander v Sweden*, above n 23.

28 *Gaskin v United Kingdom*, above n 23; *Guerra v Italy* (1998) 26 EHRR 357; *McGinley and Egan v United Kingdom* (1998) 27 EHRR 1.

29 *Leander v Sweden*, above n 23, para 74.

30 In specifically noting this point, we are grateful for material prepared by Katrine Evans, the Assistant Privacy Commissioner-Legal.

7.20 The English courts have been obliged to engage with the relationship between the right to privacy expressed in Article 8 and the protection of freedom of expression guaranteed in Article 10 of the ECHR. For instance, in *In re S (a child) (Identification: restrictions on publication)* the House of Lords was confronted with a set of background facts where a local newspaper had applied ex parte for a variation to a judicial order prohibiting any identification of S's name or the school he attended. The variation would have allowed the newspaper to report the criminal trial of S's mother and to refer to the names of the accused mother and S's deceased brother, and to publish photographs.[31] The judge at first instance in the Family Division varied his order in accordance with the local newspaper's application. Appeals against the judge's decision by S to the Court of Appeal and subsequently to the House of Lords failed. The House of Lords affirmed that the consequence of allowing S the sought-after prohibition on publication would be to inhibit the media in its reporting of criminal trials, at the expense of informed debate about criminal justice. Lord Steyn, in a speech with which the other presiding members of the House of Lords agreed, said:[32]

> 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.

7.21 In this respect, Gault P and Blanchard J observed in the decision of the New Zealand Court of Appeal in *Hosking v Runting* that the decisions of the European Court of Human Rights in the English context might be of assistance:[33]

> Relevant decisions from the European Court can be important in helping develop New Zealand jurisprudence: *Nicholls v Registrar of the Court of Appeal* [1998] 2 NZLR 385 at p 397 per Eichelbaum CJ. *Peck* [*v United Kingdom* [2003] ECHR 44647/98] is instructive, particularly given the similarities between the provision in art 8 of the European convention and art 17 of the international covenant and art 16 of the UNCROC.

DATA PROTECTION

7.22 As we have identified in chapters 2 and 3, the management of information about individuals has been treated as an important dimension of privacy. It has certainly received considerable attention in the international arena. Raab and Bennett have assessed the threefold overlapping functions of the relevant international instruments relating to personal data protection as follows:[34]

> They have acted as instruments of harmonization, as templates that any state or organization might use in order to fashion its own data protection policy. They have acted as exemplars, producing a progressive and inexorable desire to be within the community of nations that has adopted data protection legislation; the more states that adopt, the higher the pressure on the nonadopters. More recently, the European Directive [discussed below] has acted as a penetrative force, with significant

31 *In re S (a child) (Identification: restrictions on publication)* [2005] 1 AC 593 (HL).

32 Ibid, para 17 Lord Steyn.

33 *Hosking v Runting* [2005] 1 NZLR 1, para 53 (CA) Gault P and Blanchard J.

34 Bennett and Raab, above n 4, 113-114.

economic consequences for those businesses that rely upon the unimpeded international flow of personal information, and that cannot claim to protect those data in ways that meet the [European Union] adequacy test. By extension, the Directive has had an influence on those governments who see a need to protect their domestic industries from the possible consequences of non-compliance.

7.23 At present there is no globally-agreed set of information privacy rules or standards. Instead, there are various intersecting privacy frameworks covering a number of sub-groups within the international community of states. There are strong similarities in the principles contained in these different frameworks, but some significant differences as well. There are, however, Fair Information Principles that are common to these frameworks, albeit with variations. According to Bennett and Raab, these underlying principles hold that an organisation:[35]

must be *accountable* for all the personal information in its possession;

should *identify the purposes* for which the information is processed at or before the time of collection;

should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances);

should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes;

should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the *finality* principle);

should *retain* information only as long as necessary;

should ensure that personal information is kept *accurate, complete, and up-to-date;*

should protect personal information with appropriate *security safeguards;*

should be *open* about its policies and practices and maintain no secret information system;

should allow data subjects *access* to their personal information, with an ability to amend it if it is inaccurate, incomplete, or obsolete.

7.24 Nevertheless, there have been calls both from businesses and from national data protection authorities for a more comprehensive set of agreed international privacy rules, but so far these calls have not been taken up.[36]

35 Ibid, 12-13 (emphasis in original). See also Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006) 78-79.

36 See for example Jay Cline "It's Time for a Global Privacy Agreement" (20 November 2006) *Computerworld* www.computerworld.com (accessed 21 November 2006); Tash Shifrin "UK Official Calls for International Privacy Standards" (9 March 2007) *Computerworld* www.computerworld.com (accessed 13 March 2007); Peter Fleischer "Call for Global Privacy Standards" (14 September 2007) http://googlepublicpolicy.blogspot.com (accessed 15 September 2007); Eric Schmidt "Global Privacy Standards Needed" (18 September 2007) *Financial Times* www.ft.com (accessed 19 September 2007).

7.25 In this section we briefly touch upon the data protection frameworks of the Organisation for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC) group and the European Union (EU), as well as on international standards developed under the auspices of the International Organisation for Standardisation (ISO). In addition to the instruments associated with these bodies, there are the 1990 United Nations guidelines concerning computerised personal files, but the United Nations has not assumed a leading role in the direction of information protection and its guidelines have had less influence than other trans-national instruments.[37] There is a relatively extensive literature on these trans-national data protection instruments which ought to be resorted to for further information.[38]

Organisation for Economic Cooperation and Development (OECD)

7.26 The OECD Council adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("the Guidelines") in 1980. Developing a basis for a degree of alignment between disparate jurisdictions was an underlying objective. In 1999, Justice Kirby (who chaired the OECD expert group on privacy and is now a judge of the High Court of Australia) noted that "the fear that [the member countries of the OECD] would introduce incompatible and conflicting laws for the defence of privacy in the newly established databases of the interlinked information technologies" proved to be a major stimulant to the production of the Guidelines.[39] The preface to the Guidelines discussed the possibilities of the developing technologies around data storage and transfer:

> The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries … to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

7.27 The preface cautioned that:

> there is a danger that disparities in national legislation [sic] could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

7.28 The Guidelines apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and

37 Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review* (Office of the Privacy Commissioner, Auckland, 1998) 14.

38 Most notably, the excellent account in Bennett and Raab, above n 4, ch 4. See also Charles Bennett "Understanding Ripple Effects: The Cross-National Adoption of Policy Instruments for Bureaucratic Accountability" (1997) 10 Governance 213.

39 See Michael Kirby "Privacy Protection, a New Beginning: OECD Principles 20 Years On" (1999) 6 PLPR 25, 25. The Australian Law Reform Commission has produced a useful account of the OECD Guidelines in its *Review of Australian Privacy Law* (ALRC DP72, Sydney, 2007) 544-547.

individual liberties".[40] The "basic principles of national application" put forward by the OECD are reproduced in full below on account of their considerable and continuing effect on international data protection law.[41]

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

(a) with the consent of the data subject; or

(b) by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle: An individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) to have communicated to him, data relating to him
- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

40 Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 2.

41 These comprise paragraphs 7-14 inclusive of ibid.

(d) to challenge data relating to him and, if the challenge is successful to have data erased, rectified, completed or amended.

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

7.29 The Guidelines state that they only represent "minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties".[42] Specific exceptions to the Principles, such as national security, are included in parts two and three of the Guidelines.

7.30 A number of major information protection statutes are grounded on the principles in the OECD Guidelines, including the legislation in the United Kingdom,[43] Australia,[44] Hong Kong[45] and New Zealand.[46] Other influential developments, such as the European Directive on Data Protection (discussed below) also operate on very similar principles.

7.31 In 1985 a Declaration on Transborder Data Flows was adopted by Ministers of OECD member states with a view to engaging with the policy issues relating to "rapid technological developments in the field of information, computers and communications", which, according to the preamble to the Declaration, had generated "significant structural changes in the economies of Member countries". The significance of the Declaration is that it recognised the increasing importance of trans-border flows of information together with the diversity of those interests participating in and benefiting from such flows.

7.32 The stated intention of the Declaration was to:

1. Promote access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information;
2. Seek transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows;
3. Develop common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonized solutions;
4. Consider possible implications for other countries when dealing with issues related to transborder data flows.

7.33 In the 1990s the OECD shifted its focus to computer security,[47] but more recently it has returned its attention to privacy. In June 2007, the OECD Council adopted a *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*. This document recommended greater

42 Ibid, Guideline 6.

43 Data Protection Act 1984 (UK). This legislation was amended in 1998 in order to reflect the requirements of 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.

44 Privacy Act 1988 (Cth).

45 Personal Data (Privacy) Ordinance (cap 486) of the Hong Kong Special Administrative Region.

46 Privacy Act 1993 (NZ).

47 Bennett and Raab, above n 4, 90-91.

cooperation among member states in the enforcement of privacy laws. Specifically, it recommended that member states improve their domestic frameworks to better enable cross-border privacy enforcement cooperation; work on developing effective international mechanisms to facilitate such cooperation; provide mutual assistance in cross-border enforcement (including through notification, complaint referral, investigative assistance and information sharing); and consult with criminal law enforcement authorities, privacy officers, civil society, business and other stakeholders in order to improve cooperation in cross-border enforcement.

Asia-Pacific Economic Cooperation

7.34 The APEC group of some twenty-one economies, including New Zealand, fashioned a regionally-focused transnational set of privacy principles in November 2004. These principles, numbering ten as at August 2007, have, during their process of development, been criticised as "OECD-lite" and as a "new low standard" by members of the Asia-Pacific Privacy Charter Council, an independent collection of privacy specialists.[48] A number of jurisdictions within the APEC grouping (such as Australia, New Zealand and Hong Kong) already have extensive legal regimes addressing privacy in terms of personal information management. Certain of these municipal approaches have been characterised as having exceeded the minimum requirements of the OECD Guidelines, while other members of APEC do not have privacy or data protection regimes at all.

7.35 Given the diversity of member-state approaches, it is unsurprising that compromises arising out of negotiations influenced eventual outcomes. Hence, in 2003 Graham Greenleaf argued that:[49]

> The overall result of the *APEC Privacy Principles (Version 1)* is a weak set of privacy principles, probably better than nothing, but not what would be regarded as acceptable in Australia, [New Zealand], Canada, [Hong Kong] or Korea. Since there should not be any suggestion of "privacy protection good enough for developing countries" in an APEC instrument, the standard of protection suggested is surprisingly and unacceptably low.

7.36 Criticism of the APEC principles prompted the Asia-Pacific Privacy Charter Council to prepare a privacy charter that contained stronger principles and more demanding implementation requirements than those included in the APEC regime. An extensive draft of the charter had been completed by September 2003.[50]

48 Graham Greenleaf "Australia's APEC Privacy Initiative: The Pros and Cons of 'OECD Lite'" (2003) 10 PLPR 1; Graham Greenleaf "APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 91. Graham Greenleaf usefully presents a commentary on those principles that he believes to be missing from the APEC framework at, ibid, 104-107. See also the critique by Chris Pounder "Why the APEC Privacy Framework is Unlikely to Protect Privacy" (15 October 2007) www.out-law.com (accessed 17 October 2007).

49 Greenleaf "Australia's APEC Privacy Initiative", above n 48.

50 See www.bakercyberlawcentre.org/appcc (accessed 14 August 2007).

7.37 Clearly, however, the APEC area is one of change. While the APEC Data Privacy Subgroup is persisting with a "choice of approach" stance, which permits member jurisdictions to retain flexibility on how to apply cross-border privacy rules (CBPR), broad agreement has been obtained in 2007 on four key elements required for CBPR: self-assessment, compliance review, recognition/acceptance and dispute resolution/enforcement.[51] According to Nigel Waters:[52]

> it seems to have been accepted that the final element of dispute resolution and enforcement must ultimately be supported by a mechanism for binding decisions by a government regulator (though not necessarily a dedicated Privacy Commissioner).

7.38 In September 2007, the APEC Ministerial Meeting launched and formally adopted an APEC "Data Privacy Pathfinder" initiative, which would allow member jurisdictions to cluster into groups in order to "pilot the implementation of cooperative initiatives prior to their adoption by all APEC members".[53] Such an approach would permit certain jurisdictions "who are ready and willing to commit to move faster in specific areas to do so".[54] The Pathfinder statement notes that:[55]

> Economies have been working for the last year on implementing the APEC Privacy Framework related to cross-border transfers of personal information through instruments such as cross-border privacy rules. The goal is to create a foundation of trust that promotes accountable data flows across the region. These cross-border data flows are the currency of the digital economy that fuels growth in the information age.

7.39 The aims of the Pathfinder initiative are specified as including the promotion of "a conceptual framework of principles of how cross-border rules should work across economies, in consultation with the various parties that may be actors in the implementation and enforcement of these rules."[56] The work plan for the initiative states that "The aim of a fully operational CBPR system is to protect the personal information of an individual no matter where in the APEC region that personal information is transferred or accessed."[57]

Council of Europe and European Union

Council of Europe

7.40 In Europe (and not only within the European Union) the Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981 was a landmark document.[58] It has

51 Nigel Waters "APEC – Asia-Pacific Agrees Need for Enforcement of Privacy Model" (July 2007) *Privacy Laws and Business International Newsletter* 19. For a perspective from before 2007, see Greenleaf "APEC's Privacy Framework", above n 48, 111-113.

52 Waters, above n 51, 19.

53 Ibid.

54 Ibid.

55 *APEC Data Privacy Pathfinder* (item for Concluding Senior Officials' Meeting, Sydney, Australia, 2-3 September 2007).

56 Ibid.

57 *APEC Data Privacy Pathfinder: Proposed Work Plan* (item for Electronic Commerce Steering Group Meeting, Cairns, Australia, 29 June 2007).

58 For further discussion of the Council of Europe Convention see Bennett and Raab, above n 4, 84-87.

underlain many subsequent Council of Europe Recommendations concerning data protection, as well as the 1995 Directive (Directive 95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

7.41 The Convention was adopted in 1980 and opened for ratification in January 1981 with member states invited to ratify.[59] Article 23 of the Convention indicated that the Committee of Ministers of the Council of Europe were entitled to "invite any State not a member of the Council of Europe to accede to this convention" via a specific procedure.[60] The entry for Article 23 within the official explanatory report accompanying the Convention states that "The convention was elaborated in close co-operation with OECD and the non-European member countries of that organisation and it is in particular those countries which one had in mind when this article was drafted".[61] By 2005, thirty-eight of the Council of Europe's then forty-six member states had signed the Convention, and of those thirty-two had ratified it.[62] No non-member states had ratified.

7.42 Article 1 of the Convention states that its purpose is "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, *and in particular his right to privacy, with regard to automatic processing of personal data relating to him* ('data protection') [emphasis added]". The explanatory report to the Convention noted that "the legal protection of individuals with regard to automatic processing of personal information relating to them" was required:[63]

> in view of the increasing use made of computers for administrative purposes. Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions, which they can perform at high speed.
>
> Further growth of automatic data processing in the administrative field is expected in the coming years *inter alia* as a result of the lowering of data processing costs, the availability of "intelligent" data processing devices and the establishment of new telecommunication facilities for data transmission.

European Union – Data Protection Directive

7.43 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data has since become the most important document relating to privacy protection standards for European Union member states. The levels of potential compulsion associated with this

59 Ibid, 84-85.

60 Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data (28 January 1981) ETS 108, art 23(1).

61 See the commentary concerning Article 23 in "Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data: Explanatory Report" http://conventions.coe.int (accessed 10 December 2007).

62 Bennett and Raab, above n 4, 85. As at the time of writing, there are forty-seven member states of the Council of Europe.

63 See the introduction to "Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data: Explanatory Report", above n 61.

1995 Directive of the European Union, whether directly or indirectly, leave it as the stand-out transnational instrument in terms of actual or potential influence on the practices of third parties. Bennett and Raab have pointed out that:[64]

> The Directive was only possible because of prior agreement on data protection principles within the OECD and the Council of Europe. It attempts to rectify some of the perceived weaknesses within these instruments, especially with regard to the enforceability of data protection rules in a global economy.

7.44 Member States of the European Union have proceeded to implement Directive 95/46/EC. Thus, the United Kingdom has implemented the Directive through the enactment of the Data Protection Act 1998, which amended the 1984 legislation.

7.45 Article 3 of the Directive provides that:

> 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
>
> 2. This Directive shall not apply to the processing of personal data:
>
> · in the course of an activity which falls outside the scope of Community law, … and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
>
> · by a natural person in the course of a purely personal or household activity.

7.46 Article 6 states that:

> 1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> 2. It shall be for the controller to ensure that paragraph 1 is complied with.

64 Bennett and Raab, above n 4, 114.

7.47 The term "personal data" is defined in Article 2(a) as:

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Under Article 2(b):

> "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

The term "controller" is expressly defined in Article 2(d) as:

> the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

7.48 One minor illustration of the breadth of the European Union directive in a municipal European Union context concerned the fining of a woman named Bodil Lindqvist by the Swedish District Court for "processing personal data by automatic means" without notifying the Swedish supervisory authority for the protection of electronically transmitted data and "transferring data to third countries without authorisation and for processing sensitive personal data". She appealed against the decision to the Swedish Court of Appeal, which referred the case to the European Court of Justice. It in turn ruled that the posting of personal information, images or video clips of others without their consent violates laws based on the European Data Protection Directive. The European Court of Justice reported that Mrs Lindqvist was a catechist in her local parish and had:[65]

> set up internet pages at home on her personal computer in order to allow parishioners preparing for their confirmation to obtain information they might need. At her request, the administrator of the Swedish Church's website set up a link between those pages and that site.
>
> The [internet] pages in question contained information about the defendant and 18 colleagues in the parish, sometimes including their full names and in other cases only their first names. The defendant also described, in a mildly humorous manner, the jobs held by her colleagues and their hobbies. In many cases family circumstances and telephone numbers and other matters were mentioned. She also stated that one colleague had injured her foot and was on half time on medical grounds.
>
> The defendant had not informed her colleagues of the existence of those pages or obtained their consent, nor did she notify the Datainspektion (supervisory authority for the protection of electronically transmitted data) of her activity. She removed the pages in question as soon as she became aware that they were not appreciated by some of her colleagues.

65 Case C-101/2001 *Lindqvist* [2004] QB 1014, 1030-1031 (ECJ).

7.49 Because the data at issue concerned "health", it was sensitive under the European Union Directive. Article 4 of the Directive applies to any company that uses data processing "equipment" or "means" in the European Union, as well as to any company that may be reached consistent with international law. The Court concluded that the act of referring to various persons and identifying them by name or by other means (displaying their telephone number or information about their working conditions and pastimes) on an internet page, constituted "the processing of personal data wholly or partly by automatic means".[66] Moreover, reference to the state of health of an individual amounts to processing of data concerning health within the meaning of the 1995 directive. Such processing of personal data was viewed as not falling within the category of purely personal or domestic activities, which are outside the scope of the directive.

7.50 The above case arguably demonstrates the difficulties of developing an approach whereby certain types or forms of information are categorised as inherently "private" as opposed to others that might not be.[67] We have suggested in chapter 3 that "private facts", including "things such as the state of my health, physical and mental",[68] might warrant moral protection under the dimension of "informational privacy" – a breach would, at the very least, merit disapproval from the complainant. The assumption underlying this comment was that there would probably be general agreement that facts such as these are *usually* private. That is, one could say that there would be a "reasonable expectation" of privacy in respect of such matters. That said, there is no assurance or certainty that such material would be regarded as "private" in all cases.[69] Some matters might be notorious to strangers for a time, such as the observation that your leg is in a cast, that you are ill or that your face is bandaged.[70] We have also cautioned, however, that there is no automatic translation from a normative or moral account of privacy to a legal right to privacy.[71] Again, what this would suggest is that one should not be overly rigid about what might count as "private" in particular circumstances and one should take care not to cast the legal net too broadly.

7.51 Yet, while rigid sub-categorisation of information can be an issue, the very breadth of the concept of "personal data" is capable of generating broad legal claims of interference with "personal data", as was the case in *Lindqvist*. In the United Kingdom, much debate ensued when the English Court of Appeal narrowed the scope of "personal data" in the case of *Durant v Financial Services Authority* (2003).[72] In the course of that case the meaning of "personal data"

66 Ibid, 1032.

67 Nicole Moreham of Victoria University of Wellington has made this point to us.

68 Following the comments of John Burrows in "Invasion of Privacy – *Hosking* and Beyond" [2006] NZ Law Rev 389, 392, although Burrows is making these comments in the context of *legal* protection as opposed to a *moral* right to privacy in the first instance.

69 Hickford, above n 3, para 5: "In any given circumstance, the query ought to be whether the information in question should be able to count as worthy of moral and perhaps legal protection in various instances".

70 Having said that, it is not always apparent what the reasons underlying the observable condition or presentation might be, and people might speculate. There might be background information that is contextual and explanatory, which others cannot access.

71 See ibid, 10-12, 66-69.

72 *Durant v Financial Services Authority* [2003] EWCA Civ 1746; [2004] FSR 28.

in section 1(1) of the Data Protection Act 1998 (UK) (which implements Article 2(a) of the Directive) was addressed. Lord Justice Auld, for the court, concluded that "not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the [Data Protection] Act [1998]", adding that, "[m]ere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data".[73] This last point was clarified as follows:[74]

> Whether it does [amount to "personal data"] in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree. It seems to me that there are two notions that may be of assistance. The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second is one of focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity. A recent example is that considered by the European Court in Criminal Proceedings against Lindquist [sic], Case C-101/01 (6th November 2003), in which the Court held, at para 27, that "personal data" covered the name of a person or identification of him by some other means, for instance by giving his telephone number or information regarding his working conditions or hobbies.

7.52 The Article 29 Working Party of the European Commission, in its Opinion 4/2007, has given a very reasoned approach to a wider definition.[75] At the time of writing it is understood that the United Kingdom Information Commissioner is trying to square the circle of these two conflicting approaches.[76] It does, however, indicate the relative precariousness of the legal position. There are, therefore, ongoing discussions as to what the concept of "personal data" might cover[77] and the resolution of this debate is not yet clear in the European context.

73 Ibid, para 28.

74 Ibid. The Court characterised Michael Durant's claim as a "misguided attempt to use the machinery of the [Data Protection] Act as a proxy for third party discovery with a view to litigation or further investigation, an exercise, moreover, seemingly unrestricted by considerations of relevance" (ibid, para 30).

75 Article 29 Data Protection Working Party "Opinion 4/2007 on the Concept of Personal Data" (20 June 2007) 01248/07/EN WP 136.

76 See Information Commissioner's Office *Data Protection Technical Guidance – Determining what is Personal Data* (16 August 2007). We are grateful to Charles Raab of Edinburgh University for bringing this point to our attention.

77 See Christopher Millard and Peter Church "Tissue Samples and Graffiti: Personal Data and the Article 29 Working Party" (2007) 18 Computers and Law 27.

Extra-territorial implications: "adequacy" and market power

7.53 The extra-territorial influence or implications of Directive 95/46/EC have also been noted. This influence may be exerted over states, as we discuss in relation to the "EU adequacy" issue, or corporations, as in the case of the Microsoft "Passport" system discussed below.

7.54 The Directive has considerable extra-territorial effect by virtue of the obligation it places on Member States regarding the export of personal data. The concept of "adequacy" arises in Article 25 of the Directive, which states that:

> 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
>
> 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
>
> 3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
>
> 4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
>
> 5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
>
> 6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
>
> Member States shall take the measures necessary to comply with the Commission's decision.

7.55 Article 26(1) specifies a number of permissible derogations from Article 25 of the Directive. These derogations may be activated provided that a "transfer or set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" occurs in circumstances where:

- the data subject has given his or her consent unambiguously to the proposed transfer; or

- the transfer is necessary to fulfil a contract between the data subject and the controller, or concluded in the data subject's interest between the controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- the transfer is necessary in order to protect the data subject's vital interests; or
- the transfer is of information from a public register.

7.56 Member states are also entitled to authorise the transfer of data to a third country with "inadequate" protection within the meaning of Article 25(2) provided the data controller enters into an arrangement (a contract in particular, for example) that "adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights" (Article 26(2)).

7.57 The concept of "adequacy" has generated policy innovations in some jurisdictions beyond the European Union. In particular, the United States has secured a finding of "adequacy" for its privacy protections through the Safe Harbour Agreement with the European Commission. This agreement was a way of bridging the gap between the different approaches to privacy protection of Europe and the United States, and accommodating the fact that the United States has no comprehensive privacy laws governing the processing of personal information in the private sector.[78]

7.58 The United States Department of Commerce in consultation with the European Commission developed the "safe harbor" framework, which the European Union approved in July 2000. In essence, certifying to the "safe harbor" regime is intended to assure European Union organisations that a United States company provides "adequate" privacy protection, as defined by the Directive. Companies that subscribe to the programme commit themselves to an agreed set of seven privacy principles that may be subject to enforcement by the Federal Trade Commission in the event of any breach. Under the Federal Trade Commission Act, for instance, a company's failure to abide by commitments to implement the "safe harbor" principles might be considered deceptive and actionable by the Federal Trade Commission. The seven principles are characterised by the headings of "notice", "choice", "onward transfer", "security", "data integrity", "access" and "enforcement".

7.59 Of advantage to United States corporations are the following attributes:

- All member states of the European Union will be bound by the European Commission's finding of "adequacy".
- Companies participating in the "safe harbor" will be deemed adequate and data flows to those companies will continue.
- Member state requirements for prior approval of data transfers will be waived or approval will be automatically granted.
- Claims brought by European citizens against United States companies will be heard within the United States in accordance with United States law subject to limited exceptions.

78 Bennett and Raab, above n 4, 102, 167-169. On the different approaches to privacy in continental Europe and the United States see James Q Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale LJ 1151.

7.60 In the wake of the passage of Directive 95/46/EC, the so-called Article 29 Working Party of the European Union proposed that states whose data protection regimes met the requirements of the Directive would be admitted onto the "white list". The appraisal of whether a jurisdiction would be entered onto the "white list" or not would be based on "consideration of 'several representative cases of transfers to a particular third country"'.[79] The practical relevance of the European Union "adequacy" issue to New Zealand has been identified in one commentary as principally twofold:[80]

> The first arises in situations where a New Zealand company relies upon the provision of personal information from organisations in the EU to its operations in New Zealand. The other issue arises where a New Zealand company uses equipment in the territory of a Member State to process personal information. The first situation will be referred to as the "transborder dataflow" issue and the latter issue is what will be referred to as the "offshore EU processing" issue.

7.61 The Privacy Commissioner has recently observed that "The Privacy Act requires a couple of amendments before New Zealand might be adjudged 'adequate'."[81] At the time of writing, these statutory amendments have not occurred.

7.62 The Directive was also the basis for European Union regulators to express their anxieties to Microsoft representatives that Microsoft was collecting more data than it required for the purposes of its Passport system, which had been designed to facilitate easier navigation amongst password-protected internet sites. Microsoft had proposed the Passport regime as a solution to the increasing demand on users of the internet to recall a variety of usernames and passwords for different websites. The proposal involved registering personal identification information on one occasion with Microsoft itself and then using an allocated password and identification number to access numerous web pages. In this way, personal information associated with the user's details would be conveyed automatically, as and when necessary.

7.63 Privacy and the relative transparency of possible information sharing emerged as issues given that queries were soon raised as to whether Microsoft would retain the collected personal identification on a secure basis or how it might use such information or disclose it to third parties, if at all. Microsoft had the option of complying with the legal expectations of the European Union or of withdrawing from the European market completely. "The second option was out of the question: the European market accounts for about a third of Microsoft's sales."[82]

7.64 The European Union and Microsoft reached an agreement in January 2003 aspiring to discipline the manner in which the Passport system would manage the information of users, including the provision of more notice and increased user control over how information might be shared. Crucially, however,

---

79 Cited in Bennett and Raab, above n 4, 100.

80 See Bruce Legorburu "Why Should Kiwis Care About EU Data Protection? Observations from a Non-EU Country which has a Data Privacy Law" (2000) 6 PLPR 114.

81 Marie Shroff, Privacy Commissioner "Privacy and Sovereignty: Data Fight or Flight?" (Address to GOVIS conference, Wellington, 10 May 2007) 9.

82 Jack Goldsmith and Tim Wu *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, New York, 2006) 175.

Microsoft extended the application of these agreed terms to its global practices in respect of Passport. As Goldsmith and Wu have suggested, "The European Union regulated [Passport] on behalf of Europeans, but the effect was to govern the whole world – at least with respect to global companies that do business in Europe."[83] These commentators have suggested the relevance of significant market power, which has clear implications for New Zealand on account of its relatively limited market power.[84]

International standards

7.65 The area of international standards has supplied another influential instrument in aid of privacy protection in the form of ISO 17799, which was adopted as the security standard in December 2000. This standard emerged out of institutions within the International Organisation for Standardisation (ISO). The security standard ISO 17799 has the advantage of being internationally recognised and auditable. Based on the best information security practices of leading international businesses, it has been well received.

7.66 Work on international information technology standards focusing more specifically on privacy rather than security is continuing within the ISO and other organisations.[85] The International Conference of Data Protection and Privacy Commissioners in 2007 passed a resolution referring to a number of standards currently under development within the ISO and supporting "the development of effective and universally accepted international privacy standards". The resolution noted that standards have an important role to play, alongside data protection and privacy legislation, and that they can be a way of translating "legal requirements into concrete practices".[86]

WORLD TRADE

7.67 With informational privacy becoming an increasingly trade-related question in terms of the cross-border flow of data, for instance, it stands to reason that "it would, sooner or later, be injected into the wider panoply of issues negotiated and arbitrated within the World Trade Organisation" (WTO).[87] It appears that the General Agreement on Trade in Services (GATS) contemplates the sorts of regulation provided for in the European Directive, as Article XIV(c)(2)(ii) of GATS states that the Agreement does not preclude the adoption or enforcement of measures necessary for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data".

7.68 However, Article VI(1) provides that "In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner." On one view, any restrictions placed on the export of data

83 Ibid.

84 Ibid, 176.

85 For a fuller discussion, see Bennett and Raab, above n 4, 105-108; Colin J Bennett and Robin Bayley "'Saying what you do and Doing what you Say': Arguments and Prospects for an International Privacy Standard" (background paper for the 29th International Conference of Data Protection and Privacy Commissioners, Montreal, Canada, 25-28 September 2007).

86 "Resolution on Development of International Standards" (29th International Conference of Data Protection and Privacy Commissioners, Montreal, Canada, 25-28 September 2007).

87 Bennett and Raab, above n 4, 108; see generally their discussion at 108-111.

to a "third country" as a consequence of an alleged failure to ensure "an adequate level of protection" for personal data might be considered less than even-handed or "impartial" if another third country, with similarly poor protections, is not subject to comparable restrictions. Indeed, there might be a risk of such restrictions breaching Article II(1) of GATS, which stipulates that:

> With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country.

7.69 It is difficult to predict the implications of these provisions of GATS for personal data protection, but it is possible "that at some point, and in some context, international data protection will be tested within the WTO."[88]

PROBLEMS OF ENFORCEMENT

7.70 Trans-border data flows and the borderless nature of the internet pose difficult questions of legal enforceability. This is an issue of increasing significance, particularly in circumstances where New Zealand-based companies wish to engage in cross-border electronic exchanges of material. It also potentially arises with the posting of information relating to New Zealanders on overseas-hosted websites.

7.71 Although not concerned with privacy, the litigation involving Yahoo! Inc, Yahoo France, and the International League against Racism and Anti-Semitism suggests the potentially fraught nature of such proceedings. At issue was the hosting by US-based Internet company Yahoo! Inc of an online auction of a vast collection of Nazi memorabilia. The French Criminal Code banned any exhibition of Nazi propaganda for sale and prohibited French citizens from purchasing or possessing such material. Although Yahoo! Inc did not advertise the auction on its French site, two French groups (La Ligue Contre le Racisme et L'Antisemitisme (LICRA) and L'Union des Etudiants Juifs de France (UEJF)) brought an action in the French courts to prevent the auction taking place on any Yahoo! site.

7.72 Yahoo! Inc argued that the French Court lacked territorial competence to deal with the case because the alleged breach took place in the United States, but the Court held that it had jurisdiction because the harm would be suffered in France. The Court ordered Yahoo! Inc "to take all necessary measures to dissuade and make impossible" visits by French-based website users to the Yahoo-hosted auction service purveying Nazi paraphernalia.[89]

7.73 There were two further hearings before the French Court, which focused on the question of implementation of the first Court order. Yahoo! Inc argued that it was unable to identify where users of the website were located, and was therefore unable to block access by French users. On this basis, the argument proceeded, were Yahoo! Inc compelled to comply with French law, it would effectively deprive all global users of access to the auction and permit French law to set the controlling standard internationally. The Court sought the assistance of an expert panel, which reported that technical procedures were available that would allow the

88 Ibid, 111.

89 *La Ligue Contre le Racisme et L'Antisemitisme (LICRA) et L'Union des Etudiants Juifs de France (UEJF) v Yahoo! Inc et Yahoo France* (22 May 2000) Interim Court Order, County Court of Paris, 6.

company to effectively exclude 90 per cent of French users. Yahoo! Inc was given three months to comply or suffer a monetary penalty. Yahoo! Inc subsequently announced that it was discontinuing the auction, but this did not stop it from pursuing the matter in the United States courts.

7.74 In December 2000 Yahoo! Inc filed a suit in the Northern District of California seeking a declaration that the French Court's orders were neither recognisable nor enforceable in the United States. LICRA and UEJF filed a motion to dismiss, claiming that the District Court lacked personal jurisdiction over them. Yahoo! Inc filed a motion for summary judgment, asserting that the orders of the French Court were in breach of the guarantee of freedom of speech in the First Amendment to the United States constitution, and claiming that summary declaratory judgment would be proper given that substantial fines were accruing on a daily basis so long as Yahoo! Inc failed to comply with the orders. In addition, Yahoo! Inc argued that the French judgment and fines would only be collectible in the United States because the French Court had prohibited collection from the French subsidiary of Yahoo! Inc (Yahoo France), and Yahoo! Inc had no other assets within the French jurisdiction.

7.75 The District Court found that it could properly exercise specific jurisdiction over LICRA and UEJF, and granted Yahoo! Inc summary judgment in its favour, holding, among other things, that enforcement of the French orders in the United States would violate the First Amendment. The orders of the French Court were declared to be unenforceable within the United States.[90] Both LICRA and UEJF filed a notice of appeal. In August 2004, the United States Court of Appeals for the Ninth Circuit upheld the appeal and reversed the ruling of the District Court that it could exercise personal jurisdiction over LICRA and UEJF. The majority opinion of the United States Court of Appeals for the Ninth Circuit stated:[91]

> Yahoo! obtains commercial advantage from the fact that users located in France are able to access its website; in fact, the company displays advertising banners in French to those users whom it identifies as French. Yahoo! cannot expect both to benefit from the fact that its content may be viewed around the world and to be shielded from the resulting costs – one of which is that if Yahoo! violates the speech laws of another nation, it must wait for the foreign litigants to come to the United States to enforce the judgment before its First Amendment claim may be heard by a United States court.

7.76 In 2006, the United States Court of Appeals for the Ninth Circuit confirmed by a majority that the judgment of the District Court in late 2001 be reversed and that the case be remanded with directions to dismiss the action by Yahoo! Inc without prejudice.[92]

7.77 The pertinence of this situation to privacy is readily demonstrated by a recent complaint to the Privacy Commissioner for Personal Data in Hong Kong, which is currently subject to appeal to the Administrative Appeal Board in that jurisdiction. The email provider, Yahoo! Hong Kong Limited, was alleged to have disclosed the

90 *Yahoo! Inc v La Ligue Contre le Racisme et L'Antisemitisme* 169 F Supp 2d 1181 (ND Cal 2001).

91 *Yahoo! Inc v La Ligue Contre le Racisme et L'Antisemitisme* 379 F 3d 1120 (Fed 9th Cir 2004) 1126.

92 *Yahoo! Inc v La Ligue Contre le Racisme et L'Antisemitisme* 433 F 3d 1199 (Fed 9th Cir 2006).

personal data of a mainland journalist to a law enforcement agency in the People's Republic of China, leading to his arrest and eventual conviction for sending foreign-based websites the text of an internal Communist Party message.[93]

7.78 During the course of the investigation, Yahoo! Hong Kong Limited submitted to the Hong Kong Privacy Commissioner for Personal Data that Yahoo! Hong Kong Limited had not disclosed the data in question but rather that Yahoo! China had done so in response to an order under the law of the People's Republic of China. At the time of the disclosure, Yahoo! China was a company in the People's Republic of China wholly owned by Yahoo! Hong Kong Limited.

7.79 As such, the focus of the investigation was on finding out whether any of the journalist's personal data was disclosed by Yahoo! Hong Kong Limited; whether Yahoo! Hong Kong Limited was a data user for the purpose of the Personal Data (Privacy) Ordinance; and whether such disclosure could be exempted under section 58 of the Personal Data (Privacy) Ordinance. The Privacy Commissioner for Personal Data found that "[i]n the circumstances, … there [had] been no contravention of the requirements of the Ordinance by [Yahoo! Hong Kong Limited]" and the complaint was dismissed.[94] In arriving at this view, the Privacy Commissioner concluded that an Internet Protocol address did not meet the definition of "personal data" and there was insufficient evidence to show that Yahoo! Hong Kong Limited had disclosed the journalist's personal data.

7.80 Another major legal issue in this investigation was whether Yahoo! Hong Kong Limited was a data user. Under the Ordinance, a "data user" is defined to mean one who controls the collection, holding, processing or use of data. As Yahoo! China was wholly owned and operated by Yahoo! Hong Kong Limited at the material time, Yahoo! Hong Kong Limited had control over Yahoo! China and was held responsible for the act of Yahoo! China. Nevertheless, the disclosure by Yahoo! China was not a voluntary act. It was done in compliance with Chinese law. Hence Yahoo! Hong Kong Limited was taken to have lost "control" over the disclosure of the data in question owing to the operation of the foreign law. The Commissioner therefore found Yahoo! Hong Kong Limited not a "data user" with regard to the disclosure. Once the Commissioner came to this view, it logically followed that the act of disclosure in the People's Republic of China would fall outside the jurisdiction of the Ordinance and Yahoo! Hong Kong Limited had not violated the provisions of the Ordinance.[95]

7.81 The practical question of enforcing a judgment beyond the jurisdiction in which it was given remains, especially in circumstances where other values, such as freedom of expression, might be accorded a different weight. Nevertheless, the issue of enforceability is of continuing relevance when considering the efficacy of a legal regime in a particular jurisdiction.

---

93 Office of the Privacy Commissioner for Personal Data, Hong Kong *Report Published Under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap 486): The Disclosure of Email Subscriber's Personal Data by Email Service Provider to PRC Law Enforcement Agency* (report number R07-3619, 14 March 2007); "Yahoo 'helped jail Chinese writer'" (7 September 2005) http://news.bbc.co.uk (accessed 14 August 2007).

94 Office of the Privacy Commissioner for Personal Data, Hong Kong, above n 93, para 8.54.

95 A lawsuit against Yahoo! was subsequently filed in the United States on behalf of the Chinese journalist, seeking to hold Yahoo! responsible for passing on information to the Chinese government that led to his arrest. This lawsuit was settled out of court in November 2007: Linda Rosencrance "Yahoo, Imprisoned Chinese Journalists Settle Lawsuit" (13 November 2007) *Computerworld* www.computerworld.com (accessed 15 November 2007).

CONCLUSION

7.82 The interaction between domestic and transnational legal-policy regimes for privacy, and questions of the transnational enforceability of privacy laws, are important issues for consideration in domestic law reform projects like this Review. As Raab and Bennett have observed: "The question is not, anymore, whether data protection policy should be made at the international or the national governmental levels. It is, and must be, made at both."[96] Another relevant question is whether domestic instruments ought to be sufficiently flexible that they can be adapted relatively swiftly to respond to transnational legal developments, or whether there should always be recourse to Parliament via primary legislation. We will return to these questions in detail in later stages of the Review.

96 Bennett and Raab, above n 4, 115.

Chapter 8:
Some Privacy Issues

8.1 The privacy value can change with time, place and culture. We have seen earlier in this paper that social conditions once militated against the development of any strong sense of privacy.[1] However in more recent times changes in our conditions of living and working, and in particular the advance of technology, have made us more protective of our privacy. That change in attitude is reflected in the law, both internationally and domestically. We saw in chapter 4 that up until the last quarter of the 20th century privacy was not much articulated as a value recognised by our legal system. From a quite early time there were specific statutory provisions and rules of the common law which we might now regard as protecting privacy interests, but they were ad hoc and fragmented and in many cases protected privacy only indirectly. Their primary purpose was sometimes to protect other interests.

8.2 However, in the last quarter of the 20th century privacy became increasingly articulated in both the judgments of the courts and statute law as a value appropriate for legal protection. What had once been seen as an ethical value, if even that, has been increasingly translated into a legal one.[2] This is not the place for a disquisition on the overlap between ethics and law, but there are deep questions as to when it is time for the law to intervene in matters which have previously been seen as matters of morals and ethics, and how and why that decision is made. However, recent New Zealand statutes,[3] and the decision of the Court of Appeal in *Hosking v Runting,*[4] leave us in no doubt that the law is now well and truly involved in matters of privacy.

8.3 We saw in chapter 3 that privacy can be divided into two kinds. The first is informational privacy. This dimension is protected by rules which prohibit or limit the disclosure or other use of personal information. Such rules protect the individual against a variety of harms, including humiliation and distress. However, sometimes the disclosure of information about a person causes more than just this kind of mental hurt. Sometimes it can lead to harassment or even physical injury, sometimes to financial damage as the result of identity theft.

1 See chapter 5 above.

2 In 1972 the Younger Committee in the UK found that while privacy was undoubtedly of concern to many, if not most, people, on balance there was no need for a general law of privacy at that time: Report of the Committee on Privacy (1972) Cmnd 5012.

3 See chapter 4 above.

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

8.4 The second type of privacy is local. It recognises the personal space of individuals, and protects against intrusion into solitude and seclusion. It covers invasions into private property, surveillance by hidden cameras, and the like. This is an aspect of freedom: I cannot be truly free if my conduct is constantly constrained by the knowledge that I may be being watched.[5]

8.5 It is not always easy to separate these two types of privacy, because generally intrusion into solitude and seclusion is done with the purpose of acquiring information about the person. Sometimes publication of that information is envisaged, sometimes not. However, strictly speaking, it is the act of invading solitude and seclusion itself which constitutes this second type of infringement, rather than its relation to the acquisition of information.

BALANCING: THE RELATIVITY OF PRIVACY

8.6 There are few absolute values in the law, and privacy is certainly not one of them. As we argued in chapter 3, our expectations of privacy are relative and must always be balanced against other countervailing values. This act of balancing is particularly demanding in the privacy area, because in some contexts there is a strong public interest in the maintenance of other values which can limit or override privacy. There can be difficult questions of what can legitimately be put into the balance, and of the respective weightings to be given to rights as against other interests. We have already seen in chapter 4 the complexities involved in balancing privacy against other law enforcement values in the fraught area of search and seizure.[6] We now give further examples.

Informational privacy

8.7 As far as informational privacy is concerned it must be weighed against the important value of freedom of information. The relationship between the two is not simple. Sometimes they can be complementary.[7] For instance, I may be readier to share information with a group of people I trust if I know there are no eavesdroppers to the conversation. Likewise, people are more likely to provide information to government or other organisations if they trust those organisations not to disclose that information without their consent. However, often privacy and freedom of information are in competition: emphasis on one limits the other. That is particularly so when personal privacy and media freedom are in issue.

5 In the Boyer Lectures in 1969 Sir Zelman Cowen said: "A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars." Zelman Cowen "The Private Man" (Boyer Lecture, Australian Broadcasting Commission, 1969) 9-10, quoted in Malcolm Crompton, Federal Privacy Commissioner "Proof of ID Required? Getting Identity Management Right" (Speech to Australian IT Security Forum, 30 March 2004) 2.

6 See paras 4.98-4.104.

7 Eric Barendt "Privacy and Freedom of Speech" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 11, 23-30; Daniel J Solove *The Future of Reputation: Gossip, Rumour, and Privacy on the Internet* (Yale University Press, New Haven (Conn), 2007) 129-132.

8.8 Freedom of information has two aspects. The first is the freedom of a person to *convey* information and ideas. The emphasis is on the communicator. That aspect of the freedom can be justified in many ways. For example, it enhances the autonomy and individuality of the communicator, and contributes to the marketplace of ideas.[8] But freedom of information is wider in that it includes, secondly, the right of a person to *receive* information as well as to convey it. It is about the flow of information in the interests of both communicator and recipient. The free flow of information is crucially important in any society. It facilitates better government. Citizens will exercise their democratic rights more effectively if they know the facts about the way our governors do their job. It is also one of the most effective controls over government. James Mill put it this way:[9]

> So true is it however that the discontent of the people is the only means of removing the defects of vicious governments that the freedom of the press, the main instrument of creating discontent, is in all civilised countries among all but the advocates of misgovernment regarded as an indispensable security and the greatest safeguard of the interests of mankind.

8.9 In New Zealand the Official Information Act 1982 recognises the importance of freedom of information to democratic government. One of its purposes is set out as follows:[10]

> To increase progressively the availability of official information to the people of New Zealand in order –
>
> i) To enable their more effective participation in the making and administration of laws and policies; and
>
> ii) To promote the accountability of Ministers of the Crown and officials, –
>
> and thereby to enhance respect for the law and to promote the good government of New Zealand.

However, good citizenship involves more than just knowledge of government. It might be said generally that the more we know about our society and the people in it, the better we understand the wellsprings of human action, and the better contribution to society we ourselves will be able to make. This understanding of people and what motivates them can promote tolerance. The more we are starved of information about people, the less we understand (although it does not follow that we should therefore know about all aspects of other people's private lives).

8.10 Further, free information facilitates the conduct of commerce and thus benefits the economy.[11] The distribution of product information stimulates commercial activity and enables consumers to compare products. The availability of information

8 Stephen Sedley "Information as a Human Right" in Jack Beatson and Yvonne Cripps (eds) *Freedom of Expression and Freedom of Information: Essays in Honour of Sir David Williams* (Oxford University Press, Oxford, 2000) 239, 239-240.

9 James Mill *Essays on Government, Jurisprudence, Liberty of the Press, and Law of Nations* (1825, reprinted 1967) 18. See, generally, Grant Huscroft "Freedom of Expression" in Paul Rishworth, Grant Huscroft, Scott Optican and Richard Mahoney *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) 308, 309-311.

10 Official Information Act 1982, s 4(a).

11 See for example discussion in New Zealand Law Commission *Public Registers: Review of the Law of Privacy: Stage 2* [NZLC *Public Registers*] (NZLC IP3, Wellington, 2007) 53-54.

about consumers and their preferences assists the commercial sector to target advertising more effectively and also to cater to people's wants. The controlled supply of information is necessary, too, for the health and safety of the community. Information is also necessary to assist in the prevention and detection of crime, and the bringing of offenders to justice.

8.11 We have expanded on these matters in our report on the law of sedition, and also in our issues paper on Public Registers.[12] Freedom of information is a right guaranteed by the New Zealand Bill of Rights Act 1990. Section 14 guarantees a right of freedom of expression, but it is the two-sided right that we have preferred to describe as freedom of information. Section 14 provides:

> 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.

8.12 However, the right of freedom of information is obviously not an absolute right either. In many contexts it must be balanced against other rights, including the right to privacy. Section 5 of the Bill of Rights provides:

> Subject to section 4 of this Bill of Rights, the rights and freedoms contained in this Bill of Rights may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

8.13 This raises a problem of some theoretical difficulty, although in practice it is probably not as difficult as it seems at first. There are two possible views about the balancing of freedom of information and privacy. One view is that because freedom of expression is expressly guaranteed by the Bill of Rights Act whereas privacy is not, freedom of information is the primary value. On this view, the only question is whether in a particular situation a limitation on freedom of information is justified because of privacy considerations. The other view is that, although not *expressly* contained in the Bill of Rights Act, privacy is nevertheless an *existing* right or freedom which, by virtue of section 28, is not to be "abrogated or restricted" by reason that it has not been expressly enacted.[13] On that view both rights (freedom of information and privacy) are of equal standing, and one starts the balancing exercise with no presumption in favour of either of them. In the United Kingdom, where freedom of expression and privacy are both expressly guaranteed by the European Convention for the Protection of Human Rights and by the Human Rights Act 1998, that is the starting point. As Lord Steyn said:[14]

> 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.

---

12 New Zealand Law Commission *Reforming the Law of Sedition* (NZLC R96, Wellington, 2006) ch 3; NZLC *Public Registers*, above n 11, 49-55.

13 This approach is taken by Thomas J (dissenting) in *Brooker v Police* [2007] 3 NZLR 91, paras 214-233 (SC). In the same case Elias CJ takes a very different view: para 40.

14 *Re S (a child)* [2005] 1 AC 593, para 17 (HL) Lord Steyn (emphasis in original). See also Thomas J in *Brooker v Police*, above n 13, para 231: "I believe that the appropriate basis on which to evaluate the competing interests is to treat both the right to freedom of expression and privacy as fundamental values and accord neither presumptive or paramount status."

8.14 While the starting points for the two approaches may seem different, it is difficult to see that in the ultimate analysis they will produce any different result, given that both approaches involve what Lord Steyn refers to as an "intense focus on the comparative importance of the specific rights being claimed in the individual case".[15]

8.15 Nevertheless in particular situations the balancing of freedom of information and privacy is a far from simple exercise. There is no magic wand which will solve the problem. Different minds may sometimes differ on the appropriate balance.

Local privacy

8.16 Local privacy is a rather different case. Local privacy is to some extent itself protected by the Bill of Rights Act, section 21 of which gives the right to be secure against "unreasonable search or seizure, whether of the person, property, or correspondence or otherwise". Unreasonableness in this context has been interpreted as having close links with expectations of privacy. Indeed, that is the explanation currently preferred by the New Zealand Court of Appeal.[16] This of course covers only certain types of invasion of local privacy. Other types may incidentally amount to trespass, nuisance or other forms of traditional legal prohibition, so are legal wrongs in themselves.

8.17 It might therefore be thought that invasions of local privacy are less likely to be outweighed by other factors in any balancing process. However, this is not necessarily the case. Local privacy is not always as strongly protected as we might at first have thought. In fact some forms of invasion of local privacy are not prohibited at all: generally speaking, a person is currently free to film someone's property, even to film through the subject's window, provided this is done from a public place and the subject is not recorded in an intimate situation. Enforcement agencies also have many powers of entry, search and surveillance, although their exercise is strictly controlled.

8.18 The element of balancing can be as crucial in a case of invasion of local privacy as it can in one of informational privacy. So, even where a form of intrusion into solitude or seclusion would otherwise be prohibited, privacy considerations may sometimes be overridden if the purpose of the intrusion was to discover information which is of genuine public concern. Thus, the Broadcasting Standards Authority (BSA) found that a television channel was not in breach of its privacy standards when it secretly recorded an interview with a doctor in his consulting rooms which was concerned with allegations that he had sexually abused patients. His position as a local body councillor, and the fact that he was standing for election as Mayor, heightened the public interest in this information.[17]

Two types of balancing

8.19 Very often, then, privacy interests have to be balanced against other interests, in particular freedom of information. The exercise of this balancing process is one of crucial importance and often of considerable difficulty. It can occur in two ways and at two levels.

---

15 As demonstrated by the majority judgments in *Hosking v Runting*, above n 4. See in particular Tipping J, para 237.

16 See chapter 4 above, paras 4.98-4.104.

17 *Hart v TV3* (10 August 2000) Broadcasting Standards Authority 2000-108/113.

8.20 First, sometimes the lawmaker (in most cases Parliament) undertakes the balancing exercise in the course of formulating rules. In other words, the balancing exercise precedes the formulation of a rule which reconciles both interests in what is seen as the most appropriate way. Sometimes the interests of freedom of information prevail entirely, and the privacy interest is given no weight. This is so in the case of a number of public registers where the information in them is searchable by anyone without restraint. Until recently, for example, that was the case with the District Land Register, with the ownership of all interests in every piece of land open to public search without exception.[18] In other cases, while freedom of information is the dominant value, statutory provision is made for certain exceptions in the interests of privacy. Thus, it is now the case that victims of domestic violence are able to request that their details contained in registers which would otherwise be public be withheld from search.[19]

8.21 On other occasions the privacy value is given dominance, although in most such cases the rule provides for certain exceptions allowing the gathering of information in the public interest. A good example is the recent amendment to the Crimes Act which makes it an offence to covertly film people in intimate situations (in the bathroom, toilet or bedroom for example).[20] This is now an offence carrying heavy penalties, but there are carefully-defined exceptions in the Act itself. They exempt, for example, officers engaged in crime detection, and officials exercising functions in relation to security or safety who need to keep people under surveillance.[21] Here important public interests in the acquisition of information outweigh the privacy of the individual who is being filmed. Likewise, the Private Investigators and Security Guards Act 1974 makes it an offence for a private investigator to take a photograph of any person without their consent, but there is a defined exception which permits such photographs if they are necessary to identify a person for the purposes of serving a legal process.[22] In these cases, then, the balance is struck by the lawmaker and is captured in express rules. Nothing is left to the judgement of law enforcers or the courts, other than the occasional difficulties of statutory interpretation.

8.22 The second kind of balancing is where the responsibility for balancing is transferred by the lawmaker to those who have to apply and enforce the law. The Official Information Act 1982 uses this approach. The fundamental principle of the Act is that information held by government agencies will normally be disclosed on request unless there is a good reason for withholding it. One such reason is that the withholding is necessary to protect a person's privacy.[23] However, this privacy interest can itself be overridden if:[24]

> in the circumstances of the particular case, the withholding of that information is outweighed by other considerations which render it desirable, in the public interest, to make that information available.

18 Land Transfer Act 1952, ss 45, 45A, 46. See also NZLC *Public Registers*, above n 11, 19.

19 Domestic Violence Act 1995, ss 108-116.

20 Crimes Act 1961, ss 216G-216N, added in 2006.

21 Crimes Act 1961, s 216N.

22 Private Investigators and Security Guards Act 1974, s 52.

23 Official Information Act 1982, s 9(2)(a).

24 Official Information Act 1982, s 9(1).

8.23 The same approach has been adopted by the Court of Appeal in the common law case of *Hosking v Runting*,[25] which decided that it is an actionable tort to publicise private facts about a person if that publicity is highly offensive. Nevertheless, it is a defence if publication is justified by a legitimate public concern in the information. The Broadcasting Standards Authority recognises the same defence in its privacy principles.[26] In these cases the lawmaker has left the difficult balancing exercise to those who apply and enforce the law. They must decide, on the facts of a particular case, whether in all the circumstances the desirability of publication outweighs the privacy interest of the person concerned. This call must be made in the first instance by those whose job it is to abide by the law: a government agency in the case of the Official Information Act, the news editor in the case of the privacy tort and the BSA principles. But that judgement can be gainsaid if the matter is appealed, or becomes the subject of legal action. An Ombudsman may disagree with the government agency's interpretation. A judge may disagree with the news editor. They often do.

8.24 Courts are not unused to this process. It has long been familiar in the law of breach of confidence, and recent developments in the law of privilege in defamation suggest that a similar exercise will have to be undertaken there.[27] Judges have made it clear that they will be the deciders of what the public interest requires. They are not prepared to let the media decide this for themselves, because as an English judge said, the media are particularly vulnerable to the error of confusing the public interest with their own interest.[28] Nor are they prepared to let the public itself decide what it wants to read or hear. The test is what it is of public *concern* to publish, not what is of public *curiosity*.[29] There is no closed list of matters which it is in the public interest to make known. In each case it is a question of balancing the relative strengths of the two interests. The weaker the case for disclosure, the weaker the privacy interest will need to be to override it.

8.25 Such an exercise places a considerable burden on the decision-maker to divine what the public interest requires. The balance arrived at may vary with time and place. In marginal cases there may also be considerable room for disagreement.[30]

8.26 Privacy is not an absolute interest, therefore, but neither are the countervailing interests – in particular freedom of information – which may require to be balanced against it. Achieving a satisfactory outcome is one of the law's more difficult questions.

---

25 *Hosking v Runting*, above n 4.

26 Broadcasting Standards Authority, Privacy Principle 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."

27 *Lange v Atkinson* [2000] 3 NZLR 385 (CA); *Jameel v Wall Street Journal Sprl* [2007] 1 AC 359 (HL).

28 Donaldson MR in *Francome v Mirror Group Newspapers* [1984] 1 WLR 892, 898. See also Tipping J in *Hosking v Runting*, above n 4, para 258: "The right to freedom of expression is sometimes cynically invoked in aid of commercial advantage."

29 This is emphasised by the majority judges in *Hosking v Runting*, above n 4: see especially Gault P and Blanchard J, para 133.

30 See for example, *Brown v Attorney-General* [2006] DCR 630 (DC), and *X v Y* [1988] 2 All ER 648.

8.27 In the rest of this chapter we introduce a number of topics which raise hard privacy questions. Some of them demonstrate the unsettled parameters of privacy; some of them are illustrations of how difficult the balancing process can be. All of them are matters of practical significance. We do not attempt to provide answers at this stage. We shall return to some of these topics in later stages of this Review.

PERSONS

8.28 The point has already been made that there are many variables in the privacy equation. One of them is the category of person whose privacy is alleged to have been invaded. Children and young persons may have different attitudes to privacy than their elders, and are generally regarded as being more vulnerable. We discuss this issue as it relates to media coverage later in this chapter. We have also discussed elsewhere in this paper the impact of cultural differences on attitudes to privacy, particularly in relation to Māori.[31] We referred to the view of some Māori that the privacy of information belonging to Māori groups (rather than individuals) may require protection.

8.29 In this section we raise the question of whether two categories of "person" have privacy interests at all: deceased persons and corporations.[32] This inquiry goes to the heart of what privacy is. It has been suggested, in the context of the tort of invasion of privacy, that respect for human dignity is an important foundation of privacy,[33] and that "The harm to be protected against is in the nature of humiliation and distress."[34] If this is so, there is a question as to whether privacy should have application to these two categories of person. The fact that this question is not answered consistently is further demonstration that we do not have a clear vision of the concept of privacy itself. Perhaps the term has different connotations in different contexts.

Deceased persons

8.30 Our statute law is inconsistent as to whether deceased persons can have "privacy". In the Privacy Act 1993 "personal information" is defined as information about an identifiable individual; "individual" is defined to mean a natural person "other than a deceased natural person".[35] The Broadcasting Act 1989 has since the year 2000 adopted this definition for the purposes of its privacy standard.[36]

31 See chapter 5 above.

32 For further discussion of privacy and deceased persons see Paul Roth "What is Personal Information?" (2002) 20 NZULR 40, 47-48; Paul Roth "Privacy Proceedings and the Dead" (2004) 11 PLPR 50; Timothy Pitt-Payne "Mother, I Sue Dead People" (2007) 157 NLJ 1532; Australian Law Reform Commission *Review of Australian Privacy Law* (ALRC DP72, Sydney, 2007) 122-136, 219-233. On corporations/legal persons and privacy see Douwe Korff *Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons* (report for the Commission of the European Communities, 1998); Lee A Bygrave "A Right to Privacy for Corporations? Lenah in an International Context" (2001) 8 PLPR 130; Carolyn Doyle and Mirko Bagaric "The Right to Privacy and Corporations" (2003) 31 ABLR 237; Norman Witzleb "The Protection of Corporations from Intrusive Media: A German Perspective" (2006) 13 Murdoch University Electronic Journal of Law 77; South African Law Reform Commission *Privacy and Data Protection* (SALRC DP 109, Pretoria, 2005) ch 3, 4-14. On privacy and organisations and groups generally see Alan F Westin *Privacy and Freedom* (Atheneum, New York, 1967) 42-51; IN Walden and RN Savage "Data Protection and Privacy Laws: Should Organisations be Protected?" (1988) 37 ICLQ 337; Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) chs 9-15.

33 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (Lenah Game Meats)* (2001) 208 CLR 199, para 43 (HCA) Gleeson CJ.

34 *Hosking v Runting*, above n 4, para 128 Gault P and Blanchard J.

35 Privacy Act 1993, s 2(1).

36 Broadcasting Act 1989, s 2(1), definition of "individual" added in 2000.

8.31 Yet other provisions of the Privacy Act appear to be at odds with this. The full definition of "personal information" in the Act is as follows (emphasis added):

> Personal information means information about an identifiable individual, *and includes information relating to a death* that is maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995 or any former Act.

Section 29(1)(a) of the Privacy Act provides that an agency may decline to disclose information requested by persons about themselves if the disclosure "would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual". Moreover, section 46(6) provides that, for the purposes of issuing under the Act any code of practice relating to health information, information privacy principle 11 (on the disclosure of personal information) shall be read as if it applies to health information about both living and deceased individuals.[37] Even though these provisions do not use the word "privacy", they clearly envisage that there is some information about deceased persons which is sensitive enough to merit protection.

8.32 The Official Information Act 1982 is much more direct. It does assume that deceased persons can have privacy. Section 9 provides that one of the good reasons for withholding official information is that the withholding is necessary to protect "the privacy of natural persons, including that of deceased natural persons."[38]

8.33 The case law, such as it is, is not much help. While the preponderance of the United States authorities hold that the right of privacy is personal to a living person, there are nevertheless a few cases holding that a close relative of the deceased may sometimes be able to sue to protect that person's memory as well as to recover for their own hurt feelings.[39] Even before the Broadcasting Act was amended in 2000, the Broadcasting Standards Authority took the view that the right to privacy only protected the living. Persons complaining about television footage of fatal crashes were unsuccessful in their complaints to the BSA.[40]

8.34 Our statutes therefore are unhelpful and confusing on this subject. The case law is also of little help.

8.35 When one looks at the question from first principles, there is no doubt that most of us would find distasteful, offensive or otherwise unacceptable, the disclosure of certain information about a deceased person. Examples would include photographs of a dead person showing the injuries from which they died; the intimate health records of a dead person; details of the bank account of a person who has recently died. There must surely be general agreement that such information should not automatically enter the public domain just because the person is dead. Is this, however, a privacy issue? We recoil at photographs of a

37 The Health Information Privacy Code 1994 provides, in respect of a deceased individual who has been dead for not less than 20 years, that a health agency must not disclose health information unless it believes that the disclosure is to, or is authorised by, the individual's representative; or that the information concerns only the fact of death and is made by and to an appropriate person (as specified in the Code); or that certain other exceptions apply: r 11, especially 11(1)(a)(ii), 11(1)(b)(ii), 11(1)(f), 11(6).

38 Official Information Act 1982, s 9(2)(a).

39 David Elder *Privacy Torts* (Thomson West, Eagen (Minn), 2002) para 1.3.

40 See for example *Halliwell v TVNZ* (23 July 1998) Broadcasting Standards Authority 1998-076.

dead person for a variety of reasons: we find them personally repugnant and upsetting to ourselves; we feel they increase the distress of the family of the deceased; we also feel instinctively that they show disrespect to the dead person. In one case where the question was whether a coroner should have suppressed details about a suspicious death, Heath J spoke of "the need to preserve the reasonable privacy interests of the family of the deceased, and the dignity afforded to a human body."[41] In the case of the publication of health records, the same reasons are engaged. In both of these cases, then, we may experience a feeling that the dignity of the dead person has been affronted. The publication of bank account details may be different. It may be rather a fear of crime and identity theft that primarily concerns us there.

8.36 While we have no hesitation in condemning such publications, it is another question whether such transgressions should be treated as matters for legal redress. It is one thing to prevent their publication by injunction or suppression order. It is another to say that they should be subject to legal action for compensation by the descendants of the deceased. Intrusion into a family's grief is redressable by the BSA, but only as a breach of a broadcasting standard,[42] not as a breach of privacy; compensation is not available. It is not clear whether legal action would lie for breach of privacy at the behest of those family members. It is to be remembered that there is no action for defamation of the dead, and it would be somewhat paradoxical if the publication of true information about a person after they have died was actionable.

8.37 It might of course be different if a publication invaded the privacy of living members of the deceased's family. Perhaps insensitive *depiction* of their grief and distress might sometimes qualify. If the so-called "breach of privacy" was publication of financial information which resulted in theft and consequent financial loss to the family, the case might be even stronger for allowing them a cause of action. Yet then it is questionable whether a privacy action would be the appropriate one: breach of confidence, or even perhaps negligence, might be more appropriate.

8.38 In this paper we prefer to leave open the question of whether a right of privacy attaches to deceased persons. We acknowledge the confused state of the law on the point. As we said at the outset, this is evidence of the lack of agreement about the very concept of privacy itself.

Corporations

8.39 Do corporations have the same privacy rights as natural persons? One occasionally sees arguments that they do. The author Alan Westin thinks that:[43]

> Just as individuals need privacy to obtain release from playing social roles and to engage in permissible deviations from social norms, so organizations need internal privacy to conduct their affairs without having to keep up a "public face".

41 *Re an inquest into the death of JRF Fardell* (1 November 2006) HC AK CIV 2006-404-3638, para 53.

42 For example, Broadcasting Standards Authority, Free to Air Television Code of Broadcasting Practice, standard 6(e).

43 Westin, above n 32, 44.

Likewise in *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* Callinan J said he:[44]

> would not rule out the possibility that in some circumstances … a corporation might be able to enjoy the same or similar rights to privacy as a natural person, not inconsistent with its accountability, and obligations of disclosure, reporting and otherwise.

8.40 While the analogy with defamation must be employed with care, corporations can sue for defamation, although only in respect of real or prospective financial loss.

8.41 On this question of whether corporations have privacy rights, our legislation is less ambiguous, although there is not much of it. For the purposes of the Privacy Act 1993 an "individual" is defined as a *natural* person.[45] The Broadcasting Act 1989 adopts the same definition in respect of its privacy standard;[46] the BSA is thus unable to entertain complaints from corporations about alleged breaches of their privacy. The Official Information Act 1982 likewise protects the privacy only of natural persons.[47] However, it is worth noting that the New Zealand Bill of Rights Act 1990 does apply, "so far as practicable", for the benefit of legal persons, although privacy is not one of the rights expressly protected under that Act.[48]

8.42 Beyond that, however, there is every bit as much ambivalence about the standing of corporations as there is about deceased persons. Most of the United States authority is against the idea of corporations having privacy, although there are two cases in which limited partnerships have been allowed to sue.[49]

8.43 The United Kingdom case of *R v Broadcasting Standards Commission*[50] did hold that a corporation could lay a complaint of breach of privacy with the Broadcasting Standards Commission when a television channel secretly filmed some of its activities, but the decision is entirely dependent on the wording of the Broadcasting Act 1996 (UK), which expressly allows corporations to lay complaints. The Judges were certainly not saying that in other contexts corporations can lay claim to privacy. Indeed, Lord Mustill said:[51]

> Can a company say that it is aggrieved by an invasion of its own privacy? As a matter of ordinary language I would not have thought so…. [I]n general I find the concept of a company's privacy hard to grasp.

---

44 *Lenah Game Meats*, above n 33, para 328.

45 Privacy Act 1993, s 2(1).

46 Broadcasting Act 1989, s 2(1), definition of "individual" added in 2000.

47 Official Information Act 1982, s 9(2)(a).

48 New Zealand Bill of Rights Act 1990, s 29. See discussion of the application of the Bill of Rights Act to legal persons in Paul Rishworth "When the Bill of Rights Applies" in Paul Rishworth, Grant Huscroft, Scott Optican and Richard Mahoney *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) 70, 109-113; Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (LexisNexis, Wellington, 2005) 110-112. One of the BORA rights that legal persons may benefit from is the protection against unreasonable search and seizure in section 21.

49 Elder, above n 39, para 1.4.

50 *R v Broadcasting Standards Commission* [2001] QB 885.

51 Ibid, 900.

8.44 But it is the case of *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*[52] in the High Court of Australia which contains the fullest judicial discussion. There is a marked difference of view. The High Court left open the question of whether a tort of invasion of privacy exists in Australia, but five judges discussed whether, if it did, it could protect corporations. Gummow and Hayne JJ thought not. They noted that a corporation is an artificial person which "lacks the sensibilities, offence and injury to which provide a staple value for any developing law of privacy." They said that whatever happens with a tort of invasion of privacy it "will be to the benefit of natural, not artificial, persons".[53] Callinan J, as noted earlier, favoured the view that in some respects corporations were analogous to natural persons; he did not wish to rule out the possibility of their having privacy rights.[54] Gleeson CJ left the matter open. On the one hand he noted that there was no reason why some internal corporate communications should be any less private than those of an individual. On the other, he thought that much of what is protected by privacy is human dignity: "This may be incongruous when applied to a corporation."[55] Kirby J likewise declined to commit himself, although he noted that if the common law were to be influenced by the International Covenant on Civil and Political Rights, the article on privacy in the covenant appeared to relate only to the human individual.[56]

8.45 So again we find, as in the case of deceased persons, that there is real uncertainty about the application of privacy law to corporations. This reflects the general uncertainty of the concept of privacy itself. If it were to be decided that privacy is purely a human value, a company which sought to bring an action in respect of disclosure of its trade secrets, its internal deliberations or its confidential documents, would usually have to rely on breach of confidence. That, however, raises the difficult issue of whether that doctrine depends solely on the existence of a confidential relationship. That debate is beyond the scope of this paper.

8.46 We also note, although do not at this point explore, the related question of whether privacy can reside in an unincorporated association or community group as distinct from the individuals who comprise it. We saw in chapter 5 that this notion of a collective privacy interest is of real importance in relation to the Māori concept of privacy.[57]

52 *Lenah Game Meats*, above n 33.

53 Ibid, paras 126, 132.

54 Ibid, para 328.

55 Ibid, para 43.

56 Ibid, paras 190-191. The argument is complicated in New Zealand by the fact that the Bill of Rights Act 1990 does not expressly recognise privacy, although the rights and freedoms it does recognise can apply to artificial persons (s 29).

57 It may be relevant in this context to note Article 27 of the International Covenant on Civil and Political Rights which gives minority groups the right to enjoy their own culture.

PRIVACY AND THE MEDIA

8.47 The importance of freedom of the press needs no elaboration. In *Hosking v Runting* Anderson J spoke of freedom of expression in the context of the media:[58]

> Freedom of expression is the first and last trench in the protection of liberty. All of the rights affirmed by the NZBORA are protected by that particular right. Just as truth is the first casualty of war, so suppression of truth is the first objective of the despot. In my view, the development of modern communications media, including for example the worldwide web, has given historically unprecedented exposure of and accountability for injustices, undemocratic practices and the despoliation of human rights.

The guarantee of freedom of expression in the New Zealand Bill of Rights Act obviously includes freedom of the press. Yet that freedom, as we have seen, cannot be absolute and uncontrolled. Modern media are a commercial enterprise competing vigorously for a share of the audience. There is no doubt that in recent years their coverage has become more aggressive, and more sensational, in an effort to capture their share of the market. So it is not unreasonable that the law should place controls on freedom of the press, and it is now clear that privacy is one of those controls. However, as we shall see, these privacy controls are patchy, and in places uncertain. Uncertainty is undesirable in the media context: it constrains more than is desirable. In this section of the chapter we shall raise some of the issues. We shall deal more fully with them in later parts of this Review.[59]

Obtaining information

8.48 Various rules protecting local privacy constrain the media in their quest for information, just as they constrain everyone else. The Crimes Act prohibits the interception of private conversations and electronic communications. Telephone tapping is unlawful, and egregious following or persistent questioning of a person might in certain circumstances amount to harassment.[60] The ordinary laws of trespass prohibit unauthorised entry onto private property.

8.49 Yet these prohibitions are piecemeal and strangely incomplete. While it is unlawful to record an oral conversation unless one is a party to it, it is not unlawful to film someone without their knowledge except in an intimate situation. There is perhaps potential for the new tort of invasion of privacy to move into this area. There is also some uncertainty about the extent of some of the local privacy rules. It is, for example, unclear just when entry on to property by reporters or camera crew amounts to trespass.[61] Much depends on the original purpose of entry, which can be difficult to prove. Camera crews engaging in door-stepping, that is to say going onto property to film someone at their door, are still not at all clear about the extent of their right to do so.

58 *Hosking v Runting*, above n 4, para 267.

59 For further information on media law and regulation as it relates to privacy see John Burrows and Ursula Cheer *Media Law in New Zealand* (5 ed, Oxford University Press, Melbourne, 2005) especially ch 6; Steven Price *Media Minefield: A Journalists' Guide to Media Regulation in New Zealand* (New Zealand Journalists Training Organisation, Wellington, 2007) especially chs 5, 15, 20.

60 See chapter 4 above.

61 *TV3 Network Services Ltd v Broadcasting Standards Authority* [1995] 2 NZLR 720. See also *T & N Channel Nine Ptd Ltd v Anning* (2002) 54 NSWLR 333.

8.50 Information about government is much more readily available than it used to be. Until 1982 it was generally not available as of right. The blanket of the Official Secrets Act 1951 lay over all information possessed by organs of government. Now the presumption is the other way under the Official Information Act 1982. The openness engendered by this legislation benefits the media, and they frequently take advantage of it. There is no suggestion that the privacy exemption is used to excess.

8.51 Nor for the most part do the information privacy principles in the Privacy Act 1993 apply to the media, so long as the media are engaging in news activities.[62] Thus, they are not constrained by the principles about collection, use and dissemination of personal information. They could not do their job if they were. Yet in a few respects the Privacy Act is said to be of concern to the media.[63] Firstly, the exact boundary between "news activity," which is not caught by the Privacy Act, and other sorts of activity which in theory could be, is not crystal clear. There has been some concern expressed by broadcasters that historical footage and documentaries may not fall within the definition of "news." While that matter has yet to be fully tested, a few opinions of the Privacy Commissioner around the definition of news activity have tended to exhibit a broad view of that term.[64] The matter does not seem to be pressing.

8.52 Secondly, the state broadcasters, TVNZ and Radio New Zealand, are not exempt from all twelve of the information privacy principles. They are obliged to give access to inquirers who wish to see the information held about them under principles 6 and 7.[65] Their status as Crown entities brings the broadcasters within the philosophy of the Official Information Act. Yet it may be thought that there is an element of unfairness about this, for their private competitors are not subject to any such constraint. The state broadcasters certainly think it is unfair.

8.53 The third problem, however, is the main one. Media allege that while they are not themselves bound by the privacy principles, their sources are, and they consequently find it much more difficult to get information from those sources than in the past. Reporters wishing to verify facts for a story say they get little assistance from agencies from whom they inquire. The Privacy Act is often cited as the reason. The evidence to date is anecdotal and we are not aware of any detailed survey which would verify the extent of the problem, but the media certainly think it is a real problem. Media representatives tell us that they believe the reticence of the agencies is often unjustified, and that people are far too ready to use the umbrella of the Privacy Act as an excuse for silence whether it in fact covers the situation or not. Whether this is the fault of the design and language of the Privacy Act, or rather of mistaken interpretation or even deliberate stratagem, is unclear.

62 Privacy Act 1993, s 2(1), definition of "agency".

63 Opinions expressed in a media and privacy meeting held at the Law Commission on 3 July 2007.

64 *Talley Family v National Business Review* (1997) 4 HRNZ 72 (CRT); *Privacy Commissioner Casenote 38197* [2003] NZPrivCmr 24.

65 Privacy Act 1993, s 2(1), definition of "news medium". To complicate matters further, the state broadcasters may refuse requests under principle 6 in certain circumstances, where disclosure would be likely to reveal a news source: Privacy Act 1993, s 29(1)(g).

8.54 Media representatives have also told us how much they rely on public registers to verify information. Among those most widely relied on are the Births, Deaths and Marriages Register, the Companies Register, the Land Transfer Register, the Electoral Roll and the Motor Vehicle Register. If they are doing a story which involves allegations against a person or persons, their lawyers rightly advise them that if they are to minimise the risk of a defamation claim they must get their facts absolutely right. Registers are the best evidence of certain basic facts about people and their property ownership. The media also note the usefulness of such registers for makers of historical and other documentaries. They are concerned about what some of them perceive as the increasing imposition of restrictions on what used to be open access to such registers. In the Public Registers part of this Review we consider the subject in detail.

Restrictions on publication

8.55 The media, together with all other persons, are subject to statutory provisions which prohibit various kinds of publication. We have outlined these provisions in chapter 4. Most of the statutes impose criminal liability, but at least one imposes civil liability: that is the Copyright Act 1994, which confers a right on a person who has commissioned a photograph or film for private or domestic purposes not to have it published.[66]

8.56 Our media respondents also speak of what they see as a growing tendency in the courts to grant suppression of name, particularly interim suppression, to persons charged with the commission of criminal offences. The language of privacy and the dignity of the individual is now finding a place in some of the judgments in this area.[67] In other words, suppression of name is now linked with privacy to a greater extent than used to be the case. The whole question of name suppression and efficacy in the context of an uncontrolled internet is a matter of some controversy. There are two sides to this argument and the Commission takes no stand on the matter. It simply notes the fact that references to privacy and human dignity are making a greater appearance in these suppression cases than was once the case.

8.57 The most significant and talked-about development in recent years, however, has been the decision of a majority of the New Zealand Court of Appeal that there is in this country a tort of invasion of privacy.[68] It operates to impose tortious liability on a person who publicises private facts about someone in a way which is offensive, subject to a defence of public concern. Given the requirement of *publicity*, it is the media which will be most affected by this new tort. Its uncertain scope leaves them unclear as to what may or may not be caught by it. Private facts are defined as those in respect of which there is a "reasonable expectation of privacy." It is already clear that this can extend well beyond intimate personal facts such as health, sexual activity and domestic relations.[69] "Offensiveness" also invites a subjective judgement, although there

66 Copyright Act 1994, s 105.

67 For example *X v Police* (10 August 2006) HC AK CRI-2006-404-259. In *R v Wharewaka* [2005] NZAR 606, para 26 (HC) Baragwanath J said that "the dignity of the individual is a core value, indeed the fundamental value, of a civilised society." (The case involved an application to search court records.)

68 *Hosking v Runting*, above n 4.

69 See for example *Brown v Attorney General*, above n 30; *Television New Zealand Ltd v Rogers* [2007] 1 NZLR 156 (CA); *Rogers v Television New Zealand Ltd* [2007] NZSC 91.

is no doubt that some matters will be very clearly on one side of the line or the other; matters at the margin will be the subject of considerable debate. The "public concern" defence will also require an exercise of judgement which may be somewhat unpredictable. As we noted earlier, the media's protestations of public concern will sometimes be met by the response that they are more interested in their own commercial imperative than in any good the publication might do for the public.

8.58 Thus, there are uncertainties in the very texture of the tort. But its common law origins leave many other open questions. Will the tort extend to protect local privacy: will it extend, for example, to control hidden cameras? Will corporations be able to plead it? Must the plaintiff have been identified in the publication? Can a privacy claim arise in respect of false allegations? There is much working out still to be done. The uncertainty worries the media.

8.59 However, given the availability of other avenues for those with privacy complaints, it is unlikely that many tort claims will reach the courts. There is a certain irony in a plaintiff bringing a delicate privacy issue to the court, one of the most public bodies in the land. There are not many cases where the cost involved will justify it. It is likely, and the New Zealand experience so far confirms this, that most of the claims which are in fact brought will be for an injunction rather than damages. Plaintiffs are likely to feel that the best way of protecting their privacy is to stop publication before it starts, if they can get in in time. Yet injunctions are not readily available in matters involving freedom of the press. The New Zealand courts have re-asserted that in several contexts in recent years.[70] The *Hosking* court affirmed that even in privacy cases injunctions should be a rarity.[71] It remains to be seen how this will work in practice. Privacy cases differ from others in that once the matter has been published, the plaintiff's privacy, the very thing that the case was brought to protect, has been destroyed and cannot be restored. Defamation cases are different in that a damages finding for the plaintiff can itself go a considerable way to reinstating the plaintiff's damaged reputation.

8.60 We will consider this new tort in stage 3 of this Review. Whatever one's view on it – and there is room for debate both ways – the emergence of the tort is no doubt one factor in the existence of what the media report to us as a heightened awareness and sensitivity in the public about privacy issues. Most media people to whom we have spoken indicate an increased level of complaint about privacy invasion in recent times. No doubt the media's own increasingly invasive reporting style contributes to this. The rising level of legal involvement in privacy is no doubt contributing as well.

Enforcement outside the courts

8.61 Persons aggrieved by media invasions of their privacy have the opportunity of redress through avenues other than the courts. The Broadcasting Act 1989, like the Broadcasting Act 1976 before it, requires broadcasters to observe certain standards, including standards which are consistent with the privacy

70 See for example *TV3 Network Services Ltd v Fahey* [1999] 2 NZLR 129 (CA).

71 *Hosking v Runting*, above n 4, para 158 Gault P and Blanchard J, and para 258 Tipping J.

of the individual.[72] Complaints that this standard has been breached can be made directly to the Broadcasting Standards Authority, which has jurisdiction to award compensation of up to $5000. It also has the ability, although it seldom exercises it, to award other redress such as ordering a station to suspend advertising, or even broadcasting, for a period of time. It can award costs as well.

8.62 The BSA hears about 20 privacy complaints a year. It has laid down a set of privacy principles. Those principles state that disclosure of private facts which would be highly offensive to an objective reasonable person is inconsistent with individual privacy – a formulation that is very similar to the *Hosking* tort. In addition there is a principle preventing conduct which intrudes into solitude and seclusion: secret filming and recording are the main examples. As with the common law tort, public interest is a defence; so is the consent of the person concerned.[73] The BSA has built up a substantial jurisprudence in the application of these principles. Given the relative newness of the subject matter, and the relatively frequent turnover of Authority members, it is probably true that there has been a certain lack of consistency in decisions in the past, but that is no longer a strong criticism. Clear patterns of decision are developing.[74] The Authority's decisions provide illustrations of the wide range of situations in which privacy complaints can arise. While their decisions are not binding precedents, it is inevitable that the courts will refer to them, if only because there is little else to turn to.

8.63 The print media are of course not subject to the BSA's jurisdiction. Persons aggrieved by breaches of privacy in newspapers and magazines can complain to the Press Council. This is a non-statutory body which has been set up by the industry itself to hear complaints about breaches of proper standards. It is chaired by a retired judge, and is comprised of members of the public as well as industry representatives. The Press Council principles have a much briefer definition of privacy than does the BSA,[75] and it hears far fewer complaints than the BSA, which is perhaps a reflection of the fact that its existence is not as widely known.[76] Given its self-regulatory and voluntary nature, the Press Council does not impose penalties. It makes findings and expects media against which findings have been made to publish them.[77]

---

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

73 The BSA Privacy Principles are posted on the BSA website: www.bsa.govt.nz/codesstandards-privacy.php.

74 See Price, above n 59, ch 5.

75 The Press Council Privacy Principle reads:

> Everyone 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.

76 On the Press Council's approach to privacy see Price, above n 59, ch 15.

77 The Press Council has recently been reviewed: Ian Barker and Lewis Evans *Review of the New Zealand Press Council* (November 2007).

8.64 The difference between the two forms of regulation for the broadcast and print media respectively has historical origins, and dates back to a time when broadcast media needed a warrant to use the airwaves. Some say that in a modern world it is difficult to justify this separate treatment of the two types of media.[78] What is even more problematic is the fact that another form of publication – the internet – has no regulator at all.

Miscellaneous matters

8.65 Privacy poses a number of other problems for the media.

Public places

8.66 Generally speaking, if something happens in a public place it is not private. One might wonder whether there can be any restrictions on photographing such conduct, or, indeed, writing about it. The usual answer will be no. But the *Hosking* case,[79] and the Broadcasting Standards Authority in its privacy jurisdiction,[80] clearly suggest there are some exceptions to this rule. Examples often cited are the photograph of the woman whose dress is unexpectedly blown up in the wind (a real example from the US),[81] the man who is filmed attempting to commit suicide in the street (a real example from the UK),[82] and the accident victim who is photographed in a shockingly injured state.[83] It should be noted too that in the well known case of the model Naomi Campbell,[84] one aspect of her successful privacy action was that she had been photographed in a public street outside a place where she was receiving treatment for her drug problems. In other words, there is a level of humiliation and distress which justifies legal action even though the description of "private" ill fits the facts which have occurred. "Offensive" it may well be, and the law regards that element as outweighing all else.

8.67 Aside from this, however, there are as yet no indications in this country, or in England, that our law is prepared to go as far as the European courts[85] in protecting well-known persons against being photographed simply as they go about their daily business in the street. Nor is there any law against photographing young children in public places, even if their celebrity parents do not want it to happen: there are decisions in both New Zealand and the United Kingdom to

78 See Benedict Kingsbury "Complaints Against the Media: A Comparative Study" (1981) 1 Canta LR 155; Gavin Ellis "Different Strokes for Different Folk: Regulatory Distinctions in New Zealand Media" (2005) 11 Pacific Journalism Review 63.

79 *Hosking v Runting*, above n 4, para 164 Gault P and Blanchard J: "in exceptional cases a person might be entitled to restrain additional publicity being given to the fact that they were present on the street in particular circumstances." See also N A Moreham "Privacy in Public Places" (2006) 65 CLJ 606.

80 See for example *Black v The Radio Network* (21 January 1999) Broadcasting Standards Authority 1999-003 (reporting details of private conversation in the street obtained by eavesdropping).

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

82 *Peck v UK* [2003] EMLR 287 (ECHR).

83 Example given by Young J in *Bathurst City Council v Saban* (1985) 2 NSWLR 704, 707-708.

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

85 *Von Hannover v Germany* [2004] EMLR 379 (ECHR). In this case, Princess Caroline of Monaco was held to have a good claim in privacy when a series of photographs were published showing her in public shopping, in restaurants, and relaxing with her family.

this effect.[86] Nevertheless, it is fair to say that there is a level of media concern about the boundaries between those occurrences in a public place it is acceptable to cover and those it is not. At the extremes, decision is easy enough, but at the margins there are some difficult judgement calls to be made.

Consent

8.68 Consent is a defence to some types of invasion of privacy. That is certainly true of the BSA's principles, and the same position must surely apply in respect of the new tort. However, consent in the media context is a surprisingly controversial subject. There is no doubt that consent may be implied as well as expressed, but one cannot imply consent to publish everything that transpires in the course of an interview merely because one consented to that interview in the first place. Nor does consent to one type of publication necessarily imply consent to another: for example, consent to appearing in a reality television programme does not necessarily imply consent to having extracts about oneself repeatedly shown in promotions for the programme. Nor is it clear whether consent needs to be fully informed: is it enough if the consent is in a signed document which was not read by the signer, or, if read, was not properly understood by that person? There are also important issues about capacity to consent in relation to minors, persons not of sound mind, and persons with language difficulties: can others consent on their behalf? An even more difficult question is whether consent once given can be withdrawn. The answer to this last question may well depend on how much reliance on the consent there has been by editors or programme makers after it was given. So far there is little guidance on these matters.

8.69 Here, then, is another area of uncertainty. It is not always clear whether consent is necessary in the first place, and, if it is, what exactly amounts to consent. Some media err on the side of caution. That is sometimes, but not always, a good thing.

The internet

8.70 As already indicated, the internet poses problems for media law in privacy just as much as it does in other areas of the law. Much material on the internet is published by people without legal advice or editorial control. Unlike the broadcasting and print media, most internet publication is not regulated by the Broadcasting Standards Authority or Press Council.[87] It is subject to the law as much as any other publication, but the perpetrators sometimes will not be able to be readily tracked down. When they can be, they may turn out to be persons of insubstantial means. To make matters worse, they may be situated offshore, in which case legal action becomes a much less effective possibility.[88] Control of the internet poses a real problem for the international legal community.

86 *Hosking v Runting*, above n 4 (children of broadcaster Mike Hosking); and *Murray v Express Newspapers plc* [2007] EWHC 1908 (children of author JK Rowling).

87 News or current affairs websites may also be able to benefit from the news media exemption in the Privacy Act.

88 A civil action is sometimes a possibility, however: see *Dow Jones Ltd v Gutnick* (2002) 194 ALR 433. Compare *Nationwide News Pty Ltd v University of Newlands* (9 December 2005) CA 202/04.

8.71 Some believe that the presence of material on the internet renders prohibition of publication in the standard media by injunction fruitless and a waste of time. Pleas are sometimes made that injunctions or name suppressions are ineffective in the context of saturation publicity on the internet. Currently the courts do not take that view,[89] although there may be occasional cases where publicity has already become so widespread that an injunction would be unrealistic.[90]

8.72 A different concern, though, is that the uncensored and often extreme character of internet publication may over time affect the public perception of what is acceptable, and that that perception may permeate into the mainstream media. Community standards change over time, and the internet, unless it can somehow be kept in check, has the potential to change them for the worse.

Children

8.73 Children raise special privacy issues.[91] They are comparatively defenceless, and less able to give free consent than adults. The instincts of most reasonable people are that they deserve greater protection than adults. The issue is one where fairness, and a desire to further the best interests of children, come into the mix with privacy. The level of offensiveness which is an ingredient of the new tort and the BSA principles will be more readily attained in the case of children than adults. The majority in *Hosking* made special reference to the vulnerability of children.[92] The BSA has also adopted a principle that even the consent of parents and guardians to publicity about children does not exempt the broadcaster itself: it must still exercise its own judgement as to where the best interests of the child lie.[93] Broadcasters say they find that a difficult test to apply, but it does not seem an unreasonable one.

Conclusion

8.74 The media, whose job is publication, are more affected by privacy laws than most of us. We depend on them to learn what is happening around us. We have tried to show in this section that striking the balance between privacy and freedom of information is vital and difficult. The law as it currently affects the mainstream media is in some places patchy. In others it is uncertain and difficult to predict. None of these situations is ideal. Some editors who are uncertain whether they are able to publish something safely may be too cautious. Others may decide to chance it and overstep the mark. The question is whether, given the protean nature of privacy and the difficulty of capturing it in clear rules, we are going to be able to make things any better. The internet poses problems which may prove insoluble. We shall return to some of these issues at later stages of this privacy project.

89 *Re Victim X* [2003] 3 NZLR 230 (HC).

90 See for example *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716, 736 (HC) McGechan J; *Lewis Wilson & Horton Ltd* [2000] 3 NZLR 546, para 94 (CA) Elias CJ for the Court.

91 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.

92 *Hosking v Runting*, above n 4, paras 144-147.

93 BSA Privacy Principles 5, 6 and 7. See also discussion of consent, above.

PRIVACY AND THE HEALTH SYSTEM

The Context

8.75 Information is an important ingredient in good health care. The digital revolution has enabled new ways of collecting and storing health information to ensure it is available to health professionals when they need it. Computer hardware and software allow health professionals to retrieve information about a patient, and to monitor the patient's progress. In large organisations the technologies can be used to manage, standardise and monitor a whole range of tasks being carried out by the health care workforce. However, computerised data collection, storage and dissemination can give rise to significant privacy concerns. The delivery of health care can also raise complex questions about how to reconcile privacy and confidentiality with the need to share information for the benefit of the patient, or for the benefit of the wider society.

8.76 The Privacy Act 1993 applies to protect the privacy of patients. The Privacy Commissioner has issued the Health Information Privacy Code 1994 under the authority of that Act. The Code modifies the information privacy principles in relation to health information about identifiable individuals.[94] It governs the collection, holding, use and disclosure by health agencies of personal information relating to health. The Code establishes a regulatory framework for the use of personal health information, within which health practitioners can exercise discretion in accordance with their professional ethical obligations. Under the Code (as under the Act itself), patients have a right to access their own health information unless there is good reason for refusing access (for example, that disclosure may endanger the safety of any individual). There is other legislation which also deals with health information.[95]

8.77 In order to inform itself of the issues relating to health, in August 2007 the Law Commission conducted a Health Privacy Forum in conjunction with the Privacy Commissioner. Invited participants included health professionals, government officials, district health board representatives, academics, and representatives of consumer groups. In order to ensure free and frank discussion, the forum was conducted under the Chatham House rule that comments could not be attributed. We have tried to distil what we consider to be the key issues to emerge from the forum, and intend to return to these issues in the later stages of the Review.[96]

Team work and patient privacy

8.78 Sophisticated health care in a modern economy involves interactions between many different professionals: general practitioners, physicians, specialists in fields like oncology and cardiology, pathologists, dentists, radiographers, pharmacists, physiotherapists, psychiatrists, nurses and many others (including people from other sectors, such as social workers). The method is one of

94 Health Information Privacy Code 1994, cl 5.

95 In particular, sections 22B-22H of the Health Act 1956. The Public Health Bill currently before Parliament would replace these provisions: Public Health Bill 2007, no 177-1, cls 20-30. For more on the legal framework governing health information see the PDG Skegg and Ron Paterson (eds) *Medical Law in New Zealand* (Brookers, Wellington, 2006) chs 9-12.

96 For further examples and discussion of health information privacy issues see Bruce Slane "Vital Signs of Privacy: Old Verities in the New World" (address to the Royal New Zealand College of General Practitioners Conference, Rotorua, 25-29 September 2002); "Privacy and Health: How Much Should We Know?" (March 2002) *Consumer* New Zealand 14; Jodi Yeats "Sharing the Caring & Getting Privacy Right" (24 October 2007) *New Zealand Doctor* 12.

teamwork. The delivery of medical services in complex cases goes beyond the doctor-patient relationship, and privacy of patient information must be considered in this broader context. The patient's medical record is at the heart of all the activity. Each professional must have the correct information available in order to be able to function effectively and quickly. The clinical records of the patient must be accurate and they must be available to those responsible for providing the clinical treatment to the patient at each stage in the medical system.

8.79 Members of the health professions are under stern ethical duties of patient confidentiality to protect the information about the patient they have collected. Medical practitioners are obliged to "protect the patient's private information throughout his/her lifetime and following death, unless there are overriding public interest considerations at stake, or a patient's own safety requires a breach of confidentiality".[97] But health professionals need to be able to communicate about that information between themselves. Good information quickly available can be crucial in providing medical treatment, particularly in emergencies.

The national scene

8.80 New Zealanders are accustomed to thinking they have a public health system that is publicly funded and publicly administered, but to some extent that impression is misleading. The system is highly devolved and there are many private sector participants, including doctors, pharmacists, surgeons and private hospitals. General practitioners collectively probably see a total of 50,000 people a day, far more people than are in public hospitals.

8.81 The New Zealand health system faces a number of challenges, including an ageing population that will put increasing pressure on health services; rising incidences of chronic diseases such as diabetes, cardiovascular disease and cancer; fiscal constraints; and difficulties with recruiting and retaining health professionals. In response, New Zealand has chosen to focus on population health, wellness and disease prevention, and in particular on primary health care and specific populations with identified high health needs.[98]

8.82 The role of information in the system is vital. Health information is used both to inform decisions made to maintain the effectiveness and efficiency of the health system, and to support the delivery of health services to populations and individuals.

8.83 There are five key uses of health information in the delivery of health services:

- supporting clinical intervention;
- clinical governance (including professional standards, clinical audit, team development, effective relationships, and patient and community input into service development);
- administration (in all parts of the health sector), including evaluation, quality assurance and payments/funding;
- strategy and policy development; and
- research.

97 New Zealand Medical Association, Code of Ethics, March 2002, Principle 5 www.nzma.org.nz (accessed 16 October 2007).

98 Health Information Strategy Steering Committee *Health Information Strategy for New Zealand* (Ministry of Health, Wellington, 2005) 3-4.

8.84 There are local, regional and national dimensions to health information in New Zealand. While the information required across these dimensions is not the same, sometimes the same information is used for several purposes. For example, clinical data collected at a local level can also be used for administrative purposes, such as providing figures as to how many people had their appendix removed in a given year. The identifiable clinical information held by the Ministry of Health nationally is not extensive, and much of it is for administrative purposes only. There are a number of large databases connected by the National Health Index number system. The Health Information Strategy describes the need to ensure there are appropriate flows of information between local, regional and national systems, in order to maximise the benefits for consumers and clients.[99] There are no plans in New Zealand to introduce a single electronic health record for each person. However, if people working within the health system were able to access information about an identifiable individual from across multiple data sets, this could be little different in some respects from creating a single electronic record for that individual.

The need for balance

8.85 The central issue for health information is to get a proper balance between keeping personal health information confidential on the one hand, and getting the right information to the right person at the right time on the other. It is not so much a matter of patient consent as of knowledge: of the patient being aware of how his or her information may be used. There need to be some explicit understandings as to how patient information will be used once it is collected. There is an expectation in the health sector that information will be shared, and patients need to know that. Some of the research done in New Zealand indicates that the further away from direct clinical care the information travels the greater will be the patient's objection to the release of the information. Whether the information is identifiable as relating to the particular patient or not is also very important, as is the sensitivity of the information concerned.

8.86 Work that has been done in New Zealand indicates that patients have some fundamental concerns. What is the purpose of collecting health information about me? How will it be used now, and in the future? Who will have access to the information? What is the framework for deciding on access? Who makes decisions about access?

8.87 An important issue is whether patients have any say or control over how their information will be shared. The new environment of increased electronic information comes about because there is more integrated care between primary and secondary healthcare for screening and managing chronic illness. Such systems need to be the subject of consultation. Funders are seeking more information to monitor health outcomes. There has been some recent controversy over insurance companies asking for full patient records from doctors.[100] There have also been cases of health workers inappropriately accessing patients'

99 Ibid, 12-13.

100 Kim Thomas "Christchurch Doctors Resist Insurance Firms' Pleas for Full Patient Records" (3 September 2007) *The Press* Christchurch.

records, although it is significant that it appears to be easier to detect such inappropriate access with electronic than with paper records.[101] At the same time, some people may want to have their health information online so that they, and people they authorise, can access it.[102]

Mental health and patient privacy

8.88 Mental health issues raise particularly difficult questions of patient privacy.[103] Tensions exist between sharing information about mental health patients and respecting their privacy. On the one hand, family members and care givers may need to be involved and informed; on the other hand, patients may want autonomy and independence from their family.

8.89 Issues of privacy may also extend to the wider community. For example, where a special patient has committed a serious crime, but is rehabilitated and living in the community, should his doctor tell potential employers about his mental health history? What if the patient makes confessions to a doctor of committing crimes for which he has not been tried? Should the police be told?

8.90 The key to resolving such dilemmas is good clinical decision-making by the health professionals involved. For this they need proper information, and need to know they can get it from caregivers, who in turn will need to be informed of the circumstances. A low level of understanding of often complex legal provisions may hamper best clinical practice.

Genetics

8.91 Difficult issues are emerging with genetics, some of which have been discussed in chapter 6.[104] Advances in genetics are likely to feature in all aspects of health care. Traditional models of a therapeutic relationship between one patient and one practitioner, and existing safeguards which are focussed on the individual, may need to be reconsidered in the light of genetic medicine's focus on the genetic characteristics shared by families and other related groups.

8.92 Two United States cases, often cited in the discussion of disclosure in the area of genetics, illustrate the sorts of issues that may arise. In *Pate v Threlkel*, the Supreme Court of Florida held that a physician's duty of care to the children of a patient required the physician to warn the patient of the genetically-transferable nature of the condition for which he or she is being treated, but that it is not necessary to directly warn the patient's children.[105] However the following

101 Martin Johnston "Worker Sacked for Reading Celebrities' Health Records" (20 November 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 20 November 2007).

102 For example, Microsoft now offers a free service which enables consumers to collect, store and share health information online, plus search the internet for health queries. See www.healthvault.com (accessed 16 October 2007).

103 See Mental Health Commission *Review of the Implementation of the Privacy Act 1993 and the Health Information Privacy Code 1994 by District Health Boards' Mental Health Services* (2002). In response to this review, the Ministry of Health established a project team which produced a national statement on "Expectations for Information-Sharing and Related Practices in Mental Health Services". This statement is available on the Ministry of Health website www.moh.govt.nz.

104 As noted in chapter 6 above, the Human Genome Research Project at the University of Otago will examine genetic privacy in the third year of the project, with a report to be published in 2008.

105 *Pate v Threlkel* 661 So.2d 278 (Fla 1995).

year in *Safer v Pack*,[106] the Supreme Court of New Jersey Appellate Division declined to follow the reasoning in *Pate*, and held that reasonable steps have to be taken to inform not only the patient but also those likely to be affected by a genetically-transferable disease.

Medical research

8.93 Medical research and epidemiology make a long-term contribution to positive health outcomes. There are tensions, however, between the protection of privacy and the use of personal health information for research in the public interest.[107] Anonymising personal health data or obtaining consent for use of such data are not always possible. For example, identifiable data may be needed in order to trace individuals in longitudinal studies. Obtaining consent for the use of personal health data contained in records may be impractical due to the quantity or age of the data, or the results may be biased if only the data of self-selected (rather than randomly selected) individuals are used. A report to the Minister of Health by the National Ethics Advisory Committee considered the use for research purposes of identifiable data initially collected for clinical care purposes, and the Committee subsequently produced guidelines on the use of identifiable health data for research without consent.[108] However, there remains an outstanding issue as to whether there is a strong enough public mandate for the use of personal health information without consent for research in the public good. The balance to be struck is not an easy one, but public health concerns must weigh heavily in that balance.

Conclusion

8.94 It is not possible to do justice to the manifold complexities of the health information systems in New Zealand within a short compass. Neither does the Law Commission yet hold concluded views on the subject. We do believe that health information system issues are important. They involve delicate, difficult and potentially controversial use of personal information. Most participants at our forum seemed to have confidence in the principles that drive the Privacy Act 1993 on the use of personal information. But the impression we have reached (and it is only an impression) is that the issues relating to the use of health information are so complicated, diffuse, various and of such importance to the country that it may be worth considering designing a purpose-built health information statute that lays down a clear framework as to the following issues:

- who may gather personal health information;
- who may use it, for what purposes, and under what conditions;

106 *Safer v Pack* 677 A.2d 1188 [1996].

107 For further discussion of these issues see William W Lowrance *Learning From Experience: Privacy and the Secondary Use of Data in Health Research* (Nuffield Trust, London, 2002); Academy of Medical Sciences *Personal Data for Public Good: Using Health Information in Medical Research* (London, 2006); Academy of Medical Sciences *Report of Proceedings at the Legal Symposium on* Personal Data for Public Good (London, 2007); Australian Law Reform Commission, above n 32, ch 58.

108 National Advisory Committee on Health and Disability Support Services Ethics *Review of the Current Processes for Ethical Review of Health and Disability Research in New Zealand: Report to the Minister of Health* (Ministry of Health, Wellington, 2004) 35-38; National Ethics Advisory Committee *Ethical Guidelines for Observational Studies: Observational Research, Audits and Related Activities* (Ministry of Health, Wellington, 2006) 16-17.

- how the information may be communicated within the health system, and subject to what protections;
- how the information may be held, and by whom; and
- how information may be used by health researchers.

8.95 There are many specialised issues relating to particular types of information held in the health system. There are screening and vaccination programmes, such as the National Cervical Screening Programme (which is governed by legislation),[109] and Breast Screen Aotearoa and other programmes which are not governed by specific legislation. It should be possible to design a robust and relatively clear law that deals with all the issues. This is a question to which we shall return in stage 4 of this Review.

8.96 One reason why New Zealand does well in terms of life expectancy as compared to health expenditure is that New Zealand makes good use of health information. It is important to educate the public on these issues. Cost pressures will increase. There is a risk that the complexities of the health information system mean that health experts are "flying under the radar" in the sense that the public are not always aware of what is happening. It is important to engage with the public and consumers in the health information field. Health is becoming a global market. People go abroad for medical treatment and there is an increase in telemedicine (the use of information and communications technologies to provide health care at a distance). How will the information system cope in the future with these developments? The Law Commission believes this subject is a vitally important area upon which the spotlight should be shone and an overhaul carried out. At present there is a lack of clarity.

SURVEILLANCE

8.97 The day-to-day activities of social relations, business, education and sport ensure that most people watch others to some extent. Only hermits can expect no scrutiny from others. But surveillance implies something more than casual observation: it is purposeful and focused.[110] Surveillance can be defined as a "watch kept over a person or thing."[111] While the boundaries of the concept are not altogether settled, it is clear that surveillance by a variety of technological devices is a classic infringement of local privacy. It does not necessarily require technology however: surveillance can be carried out by a person using their unaided senses. The watching itself may be the cause for concern, or it may be a prelude to the publication of information obtained by the surveillance. Thus, it can interfere with both local and informational privacy.

8.98 Law enforcement activities rely heavily on surveillance in a variety of forms. In 2007 the Law Commission produced a report on *Search and Surveillance Powers*.[112] We will discuss below the relevance of the report to the current reference. For the moment, an attempt will be made to illustrate some of the dilemmas and issues that exist in the area of surveillance outside the law enforcement context.

109 Health Act 1956, ss 112A-112ZP.

110 In addition, the Surveillance Studies Network says that surveillance is routine and systematic: Surveillance Studies Network *A Report on the Surveillance Society: Full Report* (report for the UK Information Commissioner, 2006) 4. See also the discussion of the definition of surveillance in New South Wales Law Reform Commission *Surveillance: Interim Report* (NSWLRC No 98, Sydney, 2001) 55-58.

111 C T Onions (ed) *Oxford Dictionary of Etymology* (Oxford University Press, Oxford, 1978) 890.

112 New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007).

In order to focus the discussion, and show the complexity of the subject, some hypothetical examples will be employed. As will be apparent from the examples given, the law's response to various surveillance situations is not consistent, and there are some significant gaps. We note that we are not dealing here with what is sometimes called "data surveillance" (watching people by accumulating data about them from a number of sources and bringing it all together).

8.99 This part of our research has been particularly informed by the work of the New South Wales Law Reform Commission, to whom we acknowledge our debt.[113] Surveillance can be carried out, enhanced or recorded by a bewildering array of technological devices, many of them relatively new. We have discussed a number of these devices in chapter 6. Some surveillance can be beneficial, and is acceptable, but it can also be open to abuse. It may therefore require regulation by law, and some forms of surveillance are already regulated.

Surveillance examples

Example 1: *Mr Y stands outside the home of Ms X at night in the hope of seeing her in a state of undress, and he succeeds in this aim.*

8.100 It can be presumed for present purposes that Ms X did not consent to this conduct and did not know of it. While she did not pull the curtains, it cannot be presumed from this that she was indifferent to whether she was seen or not. Ms X's home is a private place and she was not consciously giving Mr Y access to her intimate self. Arguably she would have a reasonable expectation that people will not deliberately watch her undressing in those circumstances, and her privacy is violated when someone does. At present, New Zealand law deals with the situation in the example by making it an offence. Section 30 of the Summary Offences Act 1981 prohibits a person from "peeping and peering into a dwelling house." But the offence must occur at night-time, and is subject to a defence of reasonable excuse.

Example 2: *Ms X is sun bathing on a public beach topless when Mr Y photographs her with the camera on his cell phone.*

8.101 On these facts it is unlikely that Ms X would be afforded any remedy under the present law. It can be presumed for the purposes of the example that topless sun bathing is not itself an offence in these circumstances. Ms X is in a public place and cannot have a reasonable expectation of privacy of the type she could expect at home. It is not clear that her privacy has been invaded, or if it has, that any legal relief should be available. It may be argued that she has a right not be photographed, but it seems unlikely that such a right is recognised by New Zealand law as it stands at present. Different issues arise if Mr Y sells the photograph or posts it on the internet. A complaint to the Privacy Commissioner may then be possible, depending on the circumstances.

113 *Surveillance: Interim Report*, above n 110; New South Wales Law Reform Commission *Surveillance: Final Report* (NSWLRC No 108, Sydney, 2005). See also Surveillance Studies Network, above n 110, for a general discussion of surveillance.

Example 3: *Ms X is a well known actress. She is sun bathing topless beside the swimming pool in her own garden surrounded by a high fence. Mr Y is a newspaper photographer. He climbs up a tree quite distant from her garden and with a telephoto lens takes a photograph of Ms X.*

8.102 The action here does seem to amount to an invasion of Ms X's privacy. She did not know she could be observed and had a reasonable expectation that she would not be. Sections 216G – 216N of the Crimes Act 1961 make it offence to undertake covert visual recording of a person who is in a place which in the circumstances would reasonably be expected to provide privacy, and the person is naked or engaged in intimate sexual activity or is engaged in showering, toileting or dressing. The prohibition applies to a visual recording "in any medium using any device" without the knowledge of person who is recorded. The definition in the statute includes the situation where "female breasts" are exposed.

8.103 If the photographer were a private investigator an additional offence would be committed. Section 52 of the Private Investigators and Security Guards Act 1974 makes it offence for a private investigator to take photographs, film, or make a videotape recording of another person without that person's consent.

8.104 If the picture is shown on television Ms X may be able to make a complaint to the Broadcasting Standards Authority for breach of her privacy and receive a modest compensation of up to $5000 for the breach. If it appears in the newspaper, she could complain to the Press Council. However it is unclear that she has any right of action for damages at civil law. As noted earlier in this chapter, the emerging tort of privacy is neither settled nor clear in New Zealand law. There will be much fuller treatment of it in stage 3 of the Review. Ms X might succeed in this tort, but one cannot be sure. What Ms X does in her leisure time may be the subject of legitimate public interest given her prominence. She is clearly a person well known to the public.

8.105 However, if Mr Y climbed a tree and simply watched Ms X, rather than taking a photograph of her, it is less clear that there would be any legal response to his action. If the event occurs more than once, Ms X could seek the protection of a restraining order under the Harassment Act 1997, but that Act requires a pattern of behaviour that includes doing an act specified under the legislation to another person on at least two occasions in a 12 month period.[114] It would not apply to a one-off situation.

Example 4: *Ms X is the well known actress of the previous example and she goes to the movies one evening with Mr Z. The movie theatre is in a shopping mall where Closed Circuit Television cameras are operating, installed by the operators of the mall for security purposes. When they leave the theatre late at night there are not many people around and they engage in a passionate kiss that is caught by the cameras.*

8.106 On these facts without more there may be no wrong or remedy under existing law. CCTV cameras are becoming more common in New Zealand now. They operate in shops, banks, and malls, and some local governments have them on streets to try to deter street crime. Such surveillance has become widespread in some countries:[115]

114 Section 4 of the Harassment Act 1997 provides that a specified act includes watching or loitering near a person's residence.

115 Jessica Williams *50 Facts that Should Change the World* (Icon Books, Cambridge, 2004) 227.

> Researchers estimate that in a single day, a citizen of London could expect to be filmed by more than 300 cameras on more than 30 separate CCTV systems. There are thousands of cameras watching underground train lines, and Waterloo station alone is estimated to have 250 cameras. The surveillance industry has become a multi-million pound business.

8.107 While matters have not reached such intensity in New Zealand, whether the practice should be regulated is open to question. Some doubt whether these cameras do as much to reduce crime as good street lighting would do. There are also real issues about monitoring all these cameras. On the other hand, there are reports from the United Kingdom that the web of surveillance cameras played a crucial role in allowing authorities to prevent attacks by terrorists in Scotland and London.[116] If in the example the photograph were used by a publication, then some remedy could arguably be available. The image was taken for the purpose of security, but publishing it in the media has no connection to the purpose for which it was taken.

Example 5: *Ms X is such a big star that the media want every story they can secure about her. A magazine gets someone to enter her house on a false pretext during the day when she is away and plant a listening device in her sitting room in order to capture her social conversations and make use of them for articles.*

8.108 Such an example amounts to a trespass on two grounds. The illicit entry and the planting of the listening device are both trespasses, so a civil action for damages is available. Further, the unlawful interception of private communications by means of interception devices is a crime under the Crimes Act 1961, Part 9A. A private communication is one made in circumstances that reasonably indicate that any party to it desires that the communication be confined to the parties to it. The provision links the protection to reasonable expectations of privacy. Disclosing private communications that have been unlawfully intercepted and dealing in interception devices are also offences.

Regulating surveillance

8.109 Enough has been said in the discussion of these examples to indicate that surveillance raises core privacy issues and that the legal protection available for privacy is something of a patchwork quilt. As indicated earlier, the Law Commission's report *Search and Surveillance Powers* raises a number of issues that must be borne in mind in fashioning a policy approach to protecting privacy against surveillance.[117] That report proposed a revision of the present law on the use of interception and surveillance devices by law enforcement agencies, which has implications for the present reference. The Commission found that there are constantly-evolving technologies that allow people to see, hear and smell, monitor presence upon and use of property, and intercept communications, that were unimaginable only a few years ago.

8.110 At present the only activities that are subject to regulation are the interception of communications by the police, the use of tracking devices by police and customs officers, and covert filming and interception of communications by means of an interception device. People who undertake those activities without

116 "UK Camera Security Catching on" (12 July 2007) *New Zealand Herald* Auckland B2.

117 *Search and Surveillance Powers*, above n 112, ch 11.

authorisation may be the subject of civil and criminal liability. What struck the Commission as odd was that the use of a device for visual surveillance (except for intimate visual recordings) is not regulated and no offence is committed when it is undertaken. This situation was unsatisfactory from a law enforcement point of view, and from a human rights perspective as well. The central recommendation of that part of the report is that the present rules be replaced by a generic surveillance device warrant regime covering all forms of surveillance (including audio, tracking and visual) for law enforcement purposes. The use of surveillance devices in situations that do not amount to an intrusion on reasonable expectations of privacy would not be subject to regulation. The new regime would apply to any enforcement agency that had a search warrant power and a warrant could be applied for to obtain evidential material in respect to any offence for which a search warrant could be issued.

8.111 For visual surveillance, the regime would apply to enforcement officers who observe private activity by means of visual surveillance devices. This would require a warrant to be obtained where the observation of any activity is occurring in a private building, or in the curtilage of a private building where the observation extends beyond prescribed time frames and where the parties to the activity have a reasonable expectation of privacy. There would also be a requirement to obtain a judicial warrant for law enforcement activities that interfere with reasonable expectations of privacy and that are not otherwise provided for; for example, the use of devices that sense smell.

8.112 The Commission in its *Search and Surveillance Powers* report was careful not to determine what the policy should be for the present privacy reference. It concluded that the question of whether there was a need for additional criminal or civil liability for surveillance that intrudes on privacy was beyond the scope of the report and should be considered separately.[118] These were matters naturally related to the broader review of privacy protection. So what the law should be in relation to the use of these devices by people other than law enforcement officers remains unsettled to some degree.

8.113 The Law Commission in this privacy reference remains persuaded of the validity of its recommendations so recently made in the search and surveillance reference. Those recommendations are yet to be considered by the Government. The shape of the law concerning law enforcement officers has a profound influence on what should be the appropriate shape of the remaining law governing surveillance. We do not propose to indicate a policy approach on the range of privacy protections for surveillance until the decisions on *Search and Surveillance* have been taken. Those decisions will be clear before stages 3 and 4 of this project are completed. In this study paper, we are indicating that surveillance issues are serious and demand careful consideration from the Commission.

8.114 Our preliminary conclusions on surveillance are as follows:

- surveillance raises core privacy issues;
- whether surveillance should be regulated by the criminal law and in what respects is a live issue;

118 Ibid, 327.

- whether a tort of privacy should be developed by statute or allowed to develop by the common law to protect privacy against surveillance is a live issue as well;
- there may be scope for the issue to be dealt with by the Privacy Act 1993 and the Privacy Commissioner; and
- some other means of regulation may also be available.

8.115 It is important to think carefully about the costs of intervention in policy areas like the present one. Enough has been said here to show both that the issues are important ones and that the chances of getting them wrong are substantial. Whether private litigation is an efficient regulator of such activity needs careful consideration. Prosecution of criminal offences by the Crown is quite different from private litigation brought by individuals and paid for by them. Some sorts of surveillance are required in some instances to preserve the public good. Technology has made the policy problems in the area more challenging.

WORKPLACE PRIVACY

Issues and examples

8.116 Workplace privacy has received increasing attention in recent years.[119] There has been substantial legislative activity in Australia and an important study by the Law Reform Commission of the state of Victoria.[120] There is significant overlap between workplace privacy issues and the matters discussed above in relation to surveillance. Many of the same technological issues are prominent. We believe the issues are worth some consideration in this study paper, as we will need to deal with them in stages 3 and 4 of the Review. Again, as with surveillance, we illustrate the nature of the issues by the use of examples.

Example 1: *The operator of a meat works installs hidden video cameras in the bathrooms and changing rooms at the works. The cameras record employees taking drugs in the changing rooms, and while showering.*

8.117 On the face of it, the placing of hidden cameras in places where the workers would be seen undressed appears to be a gross violation of privacy. Such behaviour could be a breach of the intimate covert filming provisions, sections 216G – 216N of the Crimes Act 1961, punishable by up to three years imprisonment. Yet use of drugs in a meat works raises issues of safety that the employer may well have a proper concern about. Many people would consider that cameras on the killing chain for safety reasons are acceptable. Such places have a multitude of sharp cutting instruments and accidents are not infrequent.

119 For further discussion of workplace privacy issues in New Zealand see John M Howells "Electronic Technology and Workplace Issues: The New Zealand Situation" (2002) 24 Comp Lab L & Pol'y J 225; Caroline Morris "Drugs, the Law and Technology: Posing some Problems in the Workplace" (2002) 20 NZULR 1; Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65; Department of Labour *Big Brother Goes to Work: Video Surveillance in the Workplace* ("Themes in Employment Law", October 2005); Paul Roth "Workplace Privacy Issues Raised by RFID Technology" (Paper presented at Privacy Issues Forum, Wellington, 30 March 2006); David Maida "Who Watches You at Work?" (28 February 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 23 March 2007). For some international perspectives see for example Kirstie Ball "Expert Report: Workplace" in Appendix 4 to Surveillance Studies Network *A Report on the Surveillance Society* (report for the UK Information Commissioner, 2006); symposium issue on "Examining Privacy in the Workplace" (2006) 66 La L Rev.

120 Victorian Law Reform Commission *Workplace Privacy: Final Report* (VLRC, Melbourne, 2005).

8.118 On a similar set of facts that occurred in New Zealand, the workers involved resigned after being caught on camera taking drugs while at work.[121] Interesting issues arise about whether the evidence would have been admissible in criminal proceedings against them. Such events raise the question of whether this type of surveillance in the workplace should be regulated as it is in some Australian states. One curious feature of the New Zealand situation is that audio surveillance of the employees in those circumstances would clearly be contrary to the Crimes Act 1961, but overt video-only surveillance would not be.

Example 2: *The operator of a bus company establishes a system of random drug and alcohol testing for its drivers.*

8.119 The most important issues relating to this example may reside in the circumstances in which the tests are carried out. Do they affect decisions made by employees out of work, by detecting consumption of drugs or alcohol taken outside work hours? How are the samples to be taken? There are issues about the taking of samples of blood and urine, which are physically and mentally intrusive, and may involve some embarrassment. In situations like this, the complexity of the law governing these issues in New Zealand becomes evident. The basic law governing labour relations is the Employment Relations Act 2000. This Act provides the framework for the employer-employee relationship. Misconduct by the employer may result in a personal grievance proceeding by the employee. But serious misconduct by the employee can amount to grounds for dismissal. It is not always easy to predict whether conduct reaches this threshold.

8.120 The Health and Safety in Employment Act 1992 imposes a general duty on employers to provide a safe and healthy work environment and requires employers to manage hazards in the workplace. Employees are under duties as well, for example not to endanger themselves or others. The use of drugs and alcohol by employees could have implications for work force safety, and testing by employers may be reasonable in some circumstances. In one New Zealand case it was held that it was reasonable to test an employee upon appointment to a safety-sensitive area, to test after accidents, and to test where there was reasonable cause to suspect impairment. It was also permissible to test randomly employees who work in safety-sensitive areas. But random testing of employees engaged in non-sensitive areas was not reasonable and therefore not permitted.[122] In all probability, in the example given, a bus driver would be regarded as working in a safety-sensitive area when driving passengers.

8.121 To complete the legal picture, discriminatory treatment by employers is covered by both the Human Rights Act 1993 and the Employment Relations Act 2000. The Privacy Act 1993, and the information privacy principles set out in the Act, regulate the collection, use and disclosure of information relating to individuals and access by those individuals to that information. The Privacy Commissioner can investigate complaints and in some cases proceedings may be taken to the Human Rights Review Tribunal. The emerging tort of privacy may also have a role to play in some workplace circumstances. The existing law is usefully brought together and discussed in a recent law review article.[123]

121 Britton, above n 119, 66, citing a media report from 2005.

122 *NZ Amalgamated Engineering Printing and Manufacturing Union Inc v Air New Zealand Ltd* [2004] 1 ERNZ 614 (Emp Ct).

123 Britton, above n 119.

Example 3: *The owner of a factory dealing with dangerous chemicals in its manufacturing processes decides to expand its occupational health and safety programme to include staff DNA testing to ascertain whether some employees have a predisposition or existing genetic condition that could be affected by the processes at the factory.*

8.122 DNA testing raises sensitive privacy issues which may need to be the subject of general regulation rather than employer choice. Questions could also arise if the employer decides to make the records available to others, for example to the police. It seems unlikely that such a potentially intrusive step could be taken without a proper public policy framework erected in advance.

Example 4: *Employer A monitors the use of the firm's computers by employees at work and finds that employee B is frequently accessing soft pornography on the internet and downloading it. He is dismissed.*

8.123 On these facts the dismissal would be lawful if the procedural safeguards were properly followed by the employer. Many employers have monitoring policies in place for use of the internet and email, and the policies are frequently made part of the employment arrangements. In any case, employers are entitled to issue instructions on how the firm's equipment is to be used. These actions may be regarded as incursions on the employee's privacy, but they are sanctioned by New Zealand law, and there is little restriction on the monitoring of employee email and internet use. One commentator argued in 1996 that "employment law in New Zealand is presently structured so that it favours – and in some cases actually promotes – intrusions into the privacy interests of employees."[124] We will need to consider whether present law arrives at the correct balance.

Australian developments

Victoria

8.124 In Victoria, the Victorian Law Reform Commission has recommended an elaborate Workplace Privacy Bill. The Commission's terms of reference concentrated on surveillance and monitoring of employees' communications, and physical and psychological testing, including drug and alcohol testing. The inquiry appears to have been the first of its kind in the world.

8.125 The Commission put forward a comprehensive scheme backed by a draft Bill.[125] The approach adopted is that employers are regulated by the legislation only to the extent to which they choose to engage in privacy-invasive acts or practices in their businesses. An employer will unreasonably breach the privacy of a worker where an act or practice is performed or carried out:[126]

- for a purpose not directly connected to the employer's business;
- in a manner that is not proportionate to the purpose for which the act or practice is undertaken;

124 Paul Roth "Privacy in the Workplace – Getting the Balance Right" (Paper presented at the Privacy Issues Forum, Christchurch, 13 June 1996) 1.

125 *Workplace Privacy: Final Report*, above n 120.

126 Ibid, xx.

- without first taking reasonable steps to inform and consult with workers;
- without providing adequate safeguards to ensure the act or practice is conducted appropriately, having regard to the obligation to not unreasonably breach workers' privacy.

8.126 The Commission recommended establishing a statutory office of workplace privacy regulator, and suggested that the Victorian Privacy Commissioner was the most appropriate body to administer the workplace privacy legislation.

8.127 The essential duty on employers under the Bill would be not to engage in any act or practice that unreasonably breaches the privacy of a worker or prospective worker when the worker or prospective worker is engaged in a work-related activity. Employers would be prohibited from acts that breach the privacy of a worker when the worker is engaged in an activity that is not a work-related activity, except with specific permission from the regulator or the Victorian Civil and Administrative Tribunal. The regime would include provision for the development of advisory, approved or mandatory codes of practice, depending on the circumstances. The proposed Act would bind the Crown.

8.128 The Bill provides for a complaints process that culminates with the Victorian Civil and Administrative Tribunal. It includes large civil penalties (up to $300,000 in the case of a body corporate or $60,000 in any other case), and provides for criminal penalties. The Bill also provides that the regulator can require the respondent to cease from engaging in any act or practice that is the subject of the complaint and "take specified action to remedy the consequences of the act or practice that is the subject of the complaint or redress any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of that act or practice".[127] The amount by way of compensation is limited to $100,000. An order could also be made that the employer publishes advertisements containing information specified in the order.

8.129 Taken as a whole, the regime proposed by the Victorian Law Reform Commission is highly elaborate by New Zealand standards, and intrusive into the employment relationship. It would be expensive to run, and would impose substantial costs on employers. The question arises as to whether the proposals are proportionate to the seriousness of the conduct being regulated, or whether some less comprehensive and less bureaucratic means of regulation could accomplish as much.

8.130 Part of what was recommended by the Victorian Law Reform Commission has been enacted. The Surveillance Device (Workplace Privacy) Act 2006 (Vic) prohibits certain uses of optical surveillance devices or listening devices "to observe, listen to, record or monitor the activities or conversations of a worker in a toilet, washroom, change room or lactation room in the workplace." It is also made an offence to knowingly communicate or publish a record of an activity or conversation recorded or monitored in the circumstances covered by the quoted section.

127 Ibid, draft Workplace Privacy Bill appended to the report, cl 47(4).

New South Wales

8.131 The Workplace Surveillance Act 2005 (NSW) is less ambitious than the Victorian Law Reform Commission's proposed Workplace Privacy Bill. Part 2 of the Act deals with notification requirements of workplace surveillance of employees. Surveillance of an employee that does not comply with Part 2 is covert surveillance, which is an offence unless the surveillance is authorised by a covert surveillance authority, given by a magistrate. Under Part 2 of the Act, surveillance cannot commence without prior notice in writing to the employee, and notices must be specific about what is proposed. Where cameras are used they must be clearly visible. Tracking surveillance of an employee cannot be carried out unless there is a notice clearly visible on the vehicle indicating that the vehicle is subject to tracking surveillance. Employees cannot be subject to surveillance by an employer using a work place surveillance device (except computer surveillance) when the employee is not at work. All surveillance of change rooms and bathrooms at the workplace is prohibited. The Act requires a policy to be notified in advance before restrictions may be placed on email and internet access. There are also restrictions on the use and disclosure of surveillance records.

8.132 The grounds for the issuing of a covert surveillance authority under the Act are closely specified. Subject to some exceptions, a magistrate must not issue a covert surveillance authority unless he or she has had regard to whether covert surveillance of the employee concerned might unduly intrude on their privacy or the privacy of any other person. There is a 30 day time limit on a covert surveillance authority. A report must be furnished to the magistrate after the authority has expired.

Conclusion

8.133 The approach of the New South Wales legislation is more direct and less bureaucratic than the suggested approach in Victoria.[128] It makes it clear on the face of the statute what can and cannot be done. The elaborate system of codes of practice which are a feature of the Victorian proposals finds no place in New South Wales. It is a style of legislation likely to be more suited to New Zealand than the Victorian proposals.

8.134 The Commission believes that workplace privacy is an issue of concern, and will need to be dealt with in stages 3 and 4 of the Review. It overlaps in many respects with the general surveillance issues that will require attention in any event. It is not the Commission's intention to cut a swathe through New Zealand employment law using privacy as the instrument. While it is hard to resist the conclusion that some fresh regulation may be needed, in our view it may not need to be extensive, and might be concentrated on the use of new technologies. We will consult with employers and trade unions on these issues in the later stages of the Review.

128 The Standing Committee of Attorneys-General is now considering the issue of workplace privacy in Australia, and has issued a consultation paper on the issue: Australian Law Reform Commission, above n 32, 112-113; Standing Committee of Attorneys-General *Workplace Privacy – Options for Reform: Consultation Paper* (2007).

OTHER ISSUES

8.135 It is not our intention here to list all of the issues that the Commission will be exploring in later stages of this Review, but we mention a few other topics that may need to be addressed, by way of illustration:

- Anecdotally, it appears that the Privacy Act is often given as a reason for refusing access to information in cases where the Act does not in fact prohibit the disclosure of that information. In many cases this is due simply to misunderstanding of the Act, particularly on the part of frontline staff who deal with public inquiries. In other cases the Privacy Act may be cited when disclosure is actually restricted by other legislation, or by principles of confidentiality or professional ethics. Sometimes organisations may deliberately hide behind the Privacy Act when they do not wish to release certain information. This phenomenon (for which the Privacy Commissioner has coined the acronym "BOTPA" – "Because of the Privacy Act") may well be due more to misunderstanding than to inherent problems with the Act, but it will need to be considered in reviewing the Act.
- There appear to be questions around the extent to which increased flexibility is required for the sharing of personal information between organisations, particularly within government. Information sharing can lead to improved decision-making and service delivery. It can help to discover fraud and other criminal activity, and can help to identify individuals or groups whose needs are not being met or who are missing out on entitlements. However, the sharing of information about a person without that person's knowledge or consent can give rise to privacy concerns. If appropriate safeguards for individual privacy are not in place, information sharing may lead to a damaging loss of public trust in organisations. Further investigation is required to determine whether the appropriate balance is being struck at present.
- The Commission has discussed direct marketing in its issues paper on public registers, and noted that it is a topic that generates significant debate.[129] Important questions in this debate include whether direct marketing is an invasion of privacy or whether it is at most an irritant, and whether restricting direct marketing would have adverse effects on the New Zealand economy. It is likely that the Commission will need to consider direct marketing issues not already covered in its review of public registers when it reviews the Privacy Act.[130]
- The Australian Law Reform Commission has given extensive consideration to privacy issues in credit reporting in its Review of the Privacy Act 1988 (Cth).[131] This is in large part because that Act includes specific provisions relating to credit reporting. No such provisions are included in New Zealand's Privacy Act; instead, the Privacy Commissioner has issued the Credit Reporting Privacy Code 2004. This Code includes a provision requiring the Privacy Commissioner to review the Code as soon as practicable after 1 April 2008.[132] The Law Commission will consider the outcomes of the Privacy Commissioner's review of the Code before deciding whether any further review of credit reporting and privacy issues is required.

129 NZLC *Public Registers*, above n 11, 61-63.

130 See the discussion of the Australian situation in Australian Law Reform Commission, above n 32, ch 23.

131 Ibid, chs 48-55.

132 Credit Reporting Privacy Code 2004, cl 3. See also Marie Shroff, Privacy Commissioner "Consumer Privacy and the Credit Industry: Collecting on a Business Asset" (Speech to New Zealand Collectors Association, 30 November 2006).

CONCLUSION

8.136 The issues we have discussed in this chapter are of topical interest. They have been selected to demonstrate, on the one hand, the contested nature of privacy, and, on the other, the necessity of balancing privacy against other interests. In each of them the outcome of the balancing process has important consequences for society as a whole. We believe that these issues require further consideration, and we shall be returning to them in the course of stages 3 and 4 of this Review.

8.137 There are many other issues which raise important privacy considerations. Some have been adverted to in the course of this paper: for instance, the many massive challenges posed by new technologies, and the increasing incidence of cross-border flows of information. All of these will feature in our subsequent work in stages 3 and 4.

8.138 We have made no recommendations in this chapter, nor indeed in any other chapters of this paper. Its purpose is to set the scene for our subsequent work.

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.