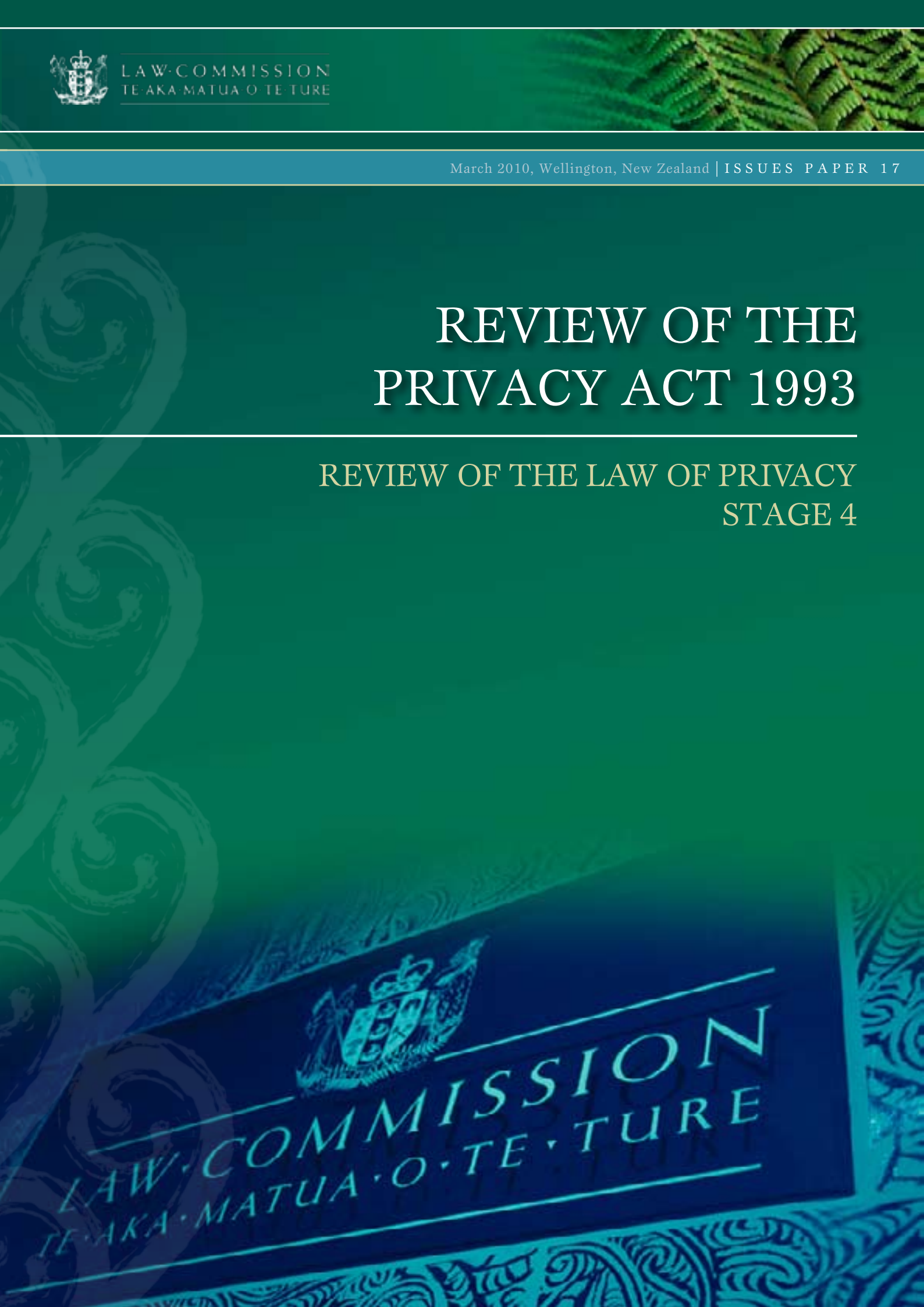
LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

March 2010, Wellington, New Zealand | ISSUES PAPER 17

REVIEW OF THE PRIVACY ACT 1993

REVIEW OF THE LAW OF PRIVACY STAGE 4



LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

March 2010, Wellington, New Zealand | ISSUES PAPER 17

REVIEW OF THE PRIVACY ACT 1993

REVIEW OF THE LAW OF PRIVACY STAGE 4

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

The Commissioners are:

Right Honourable Sir Geoffrey Palmer SC – *President*

Dr Warren Young – *Deputy President*

Emeritus Professor John Burrows QC

George Tanner QC

Val Sim

The General Manager of the Law Commission is Brigid Corcoran

The office of the Law Commission is at Level 19, HP Tower, 171 Featherston Street, Wellington

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

Document Exchange Number: sp 23534

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

Email: com@lawcom.govt.nz

Internet: www.lawcom.govt.nz

National Library of New Zealand Cataloguing-in-Publication Data

Review of the Privacy Act 1993 [electronic resource] : review of the law of privacy, stage 4.
(Law Commission issues paper ; 17)
ISBN 978-1-877316-90-6
1. New Zealand. Privacy Act 1993. 2. Privacy, Right of-
New Zealand. I. New Zealand. Law Commission.
II. Series: Issues paper (New Zealand. Law Commission : Online) ; 17

ISSN 1177-7877 (Online)
This paper may be cited as NZLC IP17
This paper is available on the Internet at the Law Commission's website: www.lawcom.govt.nz

FOREWORD

This issues paper is part of stage 4 of the Law Commission's Review of Privacy. Stage 4 is a Review of the Privacy Act 1993. We are seeking submissions from the public.

We have had to take account of a wide range of matters. The Act has been in force for 17 years, and its workings have brought to light a few problems. The international context is important too: information flows across national borders, and international treaties and conventions are increasingly important. Perhaps most importantly, technology is moving at pace and developments in computing, tracking and monitoring constantly pose challenges to our privacy.

Throughout we have had to keep in mind the crucial question of balance. On the one hand we must ensure that people's personal information is properly protected. To fail to do so can lead not just to humiliation and embarrassment but, even worse, to identity crime, stalking or reputational damage. On the other hand we must ensure that the potential of the new technologies for good is not unduly restricted, and that important values like freedom of information, health and safety and law enforcement are not impeded.

We ask a large number of questions in this paper. They range from relatively specific questions such as whether the details of the Act's privacy principles need amendment, to broader questions such as whether the Privacy Commissioner's powers need to change, to brand new questions such as whether there should be a mandatory requirement to notify breaches of privacy where data has been lost or wrongly disclosed.

On some issues the Commission has formed a provisional view and is seeking reactions to it; on others it has not yet taken a position and wants advice.

The topic has proved to be a very large one, and the issues paper is long: we could not do it justice in less. We ask many questions. We do not expect many will wish to answer all those questions. But we do hope that readers will select chapters that interest them, and let us have their views. We need all the help we can get.

Geoffrey Palmer
President
Law Commission

ACKNOWLEDGEMENTS We are grateful to the following individuals and organisations with whom we have met or corresponded in relation to this stage of our Review:

Office of the Privacy Commissioner

Ministry of Justice

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

Participants in a forum on general privacy issues held in May 2007

Participants in a consultation meeting with media representatives held in July 2007

Participants in a forum on health privacy issues held in August 2007

Participants in a meeting with privacy specialists held in May 2008

Participants in a consultation meeting with Māori held in June 2008

Australian and New South Wales Law Reform Commissions

Ministry of Health

Ministry of Social Development

New Zealand Police

Office of the Ombudsmen

Archives New Zealand

Inspector-General of Intelligence and Security

New Zealand Security Intelligence Service

Government Communications Security Bureau

State Services Commission

Trade Me

Health and Disability Commissioner

Robert Hesketh, Director of Human Rights Proceedings

Royden Hindle, Chair, Human Rights Review Tribunal

Bruce Slane

Sandra Kelman

Rowena Cullen

Call for submissions

Submissions or comments on this Issues Paper should be sent to the Law Commission by **30 April 2010.**

Privacy Submissions

Law Commission
PO Box 2590
Wellington 6140

email – privacy@lawcom.govt.nz

Any enquiries may be made to **Ewan Morris**, **04 9144 821.**

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

This Issues Paper is available on the Law Commission's website www.lawcom.govt.nz.

Official Information Act 1982

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

Review of the Privacy Act 1993

Review of the law of privacy stage 4

CONTENTS

Glossary

The following table contains a list of acronyms and abbreviations that are used regularly throughout this issues paper, and their corresponding meanings or full citations. Where appropriate, it also contains the names of some bodies and an explanation of what they do.

ALRC	Australian Law Reform Commission
APEC	Asia Pacific Economic Cooperation
Article 29 Data Protection Working Party	This is a Working Party set up under Article 29 of the EC Data Protection Directive 95/46/EC. It is an independent European advisory body on data protection and privacy.
CRPC	Credit Reporting Privacy Code 2004
DPI	Deep packet inspection
EU	European Union
Federal Trade Commission	The Federal Trade Commission is the Federal body which oversees consumer protection and competition in the US, including the regulation of business practices that impinge on personal privacy.
HIPC	Health Information Privacy Code 1994
ICO	Information Commissioner's Office (UK)
IP address	Internet Protocol address
ISP	Internet Service Provider
Necessary and Desirable	Office of the Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review* (Wellington, 1998).
1st Supplement to Necessary and Desirable	Office of the Privacy Commissioner *Supplement to first periodic review of the operation of the Privacy Act 1993: Report by the Privacy Commissioner to the Minister of Justice supplementing Necessary and Desirable: Privacy Act 1993 Review (December 1998) and offering further recommendations* (Wellington, April 2000).

2nd Supplement to Necessary and Desirable	Office of the Privacy Commissioner *Second supplement to first periodic review of the operation of the Privacy Act 1993: Report by the Privacy Commissioner to the Minister of Justice supplementing Necessary and Desirable: Privacy Act 1993 Review (December 1998) and the first supplement to that report* (Wellington, January 2003).
3rd Supplement to Necessary and Desirable	Office of the Privacy Commissioner *Third supplement to first periodic review of the operation of the Privacy Act 1993: Report by the Privacy Commissioner to the Minister of Justice supplementing Necessary and Desirable: Privacy Act 1993 Review (December 1998) and the First and Second Supplements to that report (April 2000 and January 2003)* (Wellington, December 2003).
4th Supplement to Necessary and Desirable	Office of the Privacy Commissioner *Fourth supplement to first periodic review of the operation of the Privacy Act 1993: Report by the Privacy Commissioner to the Minister of Justice supplementing Necessary and Desirable: Privacy Act 1993 Review (December 1998) and the First, Second and Third Supplements to that report* (Wellington, May 2008).
NSWLRC	New South Wales Law Reform Commission
OECD	Organisation for Economic Cooperation and Development
OIA	Official Information Act 1982 (NZ)
OPC	Office of the Privacy Commissioner (NZ)
PETs	Privacy-enhancing technologies
PIPEDA	Personal Information Protection and Electronic Documents Act 2000 (Canada)
Privacy Act	Privacy Act 1993 (NZ)
RFID	Radio frequency identification
TIPC	Telecommunications Information Privacy Code 2003
VUW report	Miriam Lips, Rose O'Neill and Elizabeth Eppel *Improving Information Sharing for Effective Social Outcomes* (Victoria University of Wellington, 2009). "VUW" is a reference to Victoria University of Wellington.

Chapter 1
Introduction

THE LAW COMMISSION'S REVIEW OF PRIVACY LAW

1.1 The Law Commission is reviewing the law relating to privacy (the Review). The Review consists of four stages. Stage 1 was a high level policy overview of privacy issues that set the conceptual framework and helped to identify issues for further detailed examination in the other stages. It resulted in the publication of the study paper *Privacy: Concepts and Issues* in January 2008.[1] The study paper did not make recommendations.

1.2 Stage 2 of the Review looked at the law relating to public registers. The Commission's final report for this stage was tabled in Parliament in February 2008.[2] The public register provisions in the Privacy Act 1993 (specifically Part 7 and Schedule 2) are therefore not dealt with in the present issues paper.

1.3 Stage 3 was concerned with the adequacy of New Zealand's civil, criminal, and regulatory law to deal with invasions of privacy, but did not focus much on the Privacy Act. The Commission published a report for stage 3 in February 2010.[3] That report looked, in particular, at the tort of invasion of privacy, remedies and penalties for surveillance, and other criminal and civil sanctions relating to invasion of privacy.

1.4 This issues paper is part of stage 4 of the Review. In this stage we will be reviewing the Privacy Act 1993.[4] The Commission's starting point for this review is an assumption, based on the work of the Privacy Commissioner and its own research, that the Privacy Act is basically sound and not in need of a major rethink. That is not to say that the Act cannot be improved. While we consider that the framework of the Act, and the principles on which it is based, are sound, we also consider that there are some very significant areas that need examination and discussion. These are dealt with in detail in later chapters of this issues paper.

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

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

3 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, Wellington, 2010).

4 Throughout this issues paper any reference to "Privacy Act" means the Privacy Act 1993 of New Zealand, unless the context suggests otherwise.

OTHER REVIEWS

Privacy Commissioner statutory reviews of the Privacy Act

1.5 Section 26(1) of the Act requires the Privacy Commissioner to review the operation of the Act as soon as practicable after it has been in force for three years, and then at intervals of not more than five years. The Commissioner must consider whether any amendments to the Act are necessary or desirable, and report his or her findings to the responsible Minister. The Minister is then required to present the Commissioner's report to the House of Representatives.

1.6 The first statutory review of the Act was started in 1997 by the then Privacy Commissioner, Bruce Slane. The outcome of that review was contained in his report to the Minister in November 1998. The report was called *Necessary and Desirable: Privacy Act 1993 Review*.[5] Mr Slane updated that report with two supplementary reports in April 2000[6] and January 2003.[7] His successor, Marie Shroff, produced further supplementary reports in December 2003[8] and May 2008.[9]

Ministry of Justice work

1.7 In *Privacy: Concepts and Issues*, we indicated that the Ministry of Justice was undertaking work on modernising the Privacy Act 1993, with a view to making a number of operational and technical amendments to the Act.[10] It was anticipated that these amendments to the Act would pick up many of the recommendations contained in *Necessary and Desirable* and the supplementary reports.

1.8 However, to have two streams of work, one in the Ministry of Justice and one in the Law Commission, running concurrently would risk overlap and would be confusing to the public. So the Government agreed in May 2008 that it would not proceed with a general Privacy Amendment Bill. Instead, it would introduce a Bill solely to address cross-border data transfers of personal information in order to ensure that New Zealand's privacy laws align more closely with the European Union Directive on the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of Such Data. This Bill is outlined below. The Government also agreed that work already undertaken on more general amendments to the Act would be taken into account as part of the Law Commission's review. This will enable public involvement to be focused on a single, major review of the Act.

1.9 The recommendations in *Necessary and Desirable* (including the supplementary reports) have been examined and taken into account in the Law Commission's review, although this issues paper does not specifically consider all of those recommendations.

5 *Necessary and Desirable* (see Glossary for full publication details).

6 *1st Supplement to Necessary and Desirable* (see Glossary for full publication details).

7 *2nd Supplement to Necessary and Desirable* (see Glossary for full publication details).

8 *3rd Supplement to Necessary and Desirable* (see Glossary for full publication details).

9 *4th Supplement to Necessary and Desirable* (see Glossary for full publication details).

10 New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) para 1.15.

Privacy (Cross-border Information) Amendment Bill 2008

1.10 The Privacy (Cross-border Information) Amendment Bill 2008 is a Government Bill that was introduced into the House on 2 July 2008. At the time of writing, the Bill is awaiting its second reading.

1.11 The Bill has two main purposes:

- to reduce the likelihood of New Zealand being used as an intermediary for the avoidance of other states' privacy laws; and
- to facilitate the cross-border enforcement of privacy laws by giving the Privacy Commissioner authority to cooperate with overseas privacy enforcement authorities in consulting on, and transferring, complaints.

1.12 Chapter 14 examines the issues of trans-border data flows, and the Bill is discussed in more detail in that context.

Australian reviews

1.13 The Australian Law Reform Commission (ALRC) began a review of the Privacy Act 1988 (Cth), the Federal law dealing with information privacy, in 2006. Its overall brief was to review the extent to which the Privacy Act 1988 (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia. The ALRC delivered its final report to the Australian federal Attorney-General on 30 May 2008.[11] At the time of writing, the Australian government had given its first stage response to the report, accepting many of its recommendations.[12]

1.14 The New Zealand Law Commission has had discussions with the ALRC during the course of its review, and the ALRC's work has been very beneficial in supplementing and aiding our research efforts. We have also had the tremendous advantage of having the ALRC's report available to us while undertaking our own review, and we have drawn on it extensively in the preparation of this issues paper.

1.15 The New South Wales Law Reform Commission (NSWLRC) and the Victorian Law Reform Commission (VLRC) have also been reviewing aspects of the law relating to privacy in those states. The NSWLRC is currently reviewing the Privacy and Personal Information Protection Act 1998 (NSW), the Health Records and Information Privacy Act 2002 (NSW), and related matters. They have released a report on *Privacy Principles*,[13] which comments on the principles recommended by the ALRC, and other issues will be covered in a subsequent report. The VLRC has chosen to focus on two specific issues: workplace privacy, and surveillance in public places. They have reported on the first issue,[14] and a report on the second is expected shortly.

---

11 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008).

12 Australian Government *First Stage Response to the Australian Law Reform Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009).

13 New South Wales Law Reform Commission *Privacy Principles* (NSWLRC R123, Sydney, 2009). The NSWLRC has also reported on another part of their Privacy reference, which is concerned with the desirability of introducing a statutory cause of action for invasion of privacy: New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC R120, Sydney, 2009).

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

BRIEF DESCRIPTION OF THE PRIVACY ACT 1993

1.16 Legislation comes into being for different reasons at different times in history. The Wanganui Computer Centre Privacy Act was enacted in 1976 because of concerns about the aggregation of personal information on the Wanganui law enforcement computer system. The Privacy Act was enacted in 1993 to balance the desire of the state to make greater use of personal information held by government agencies, especially for data matching, with the need to protect the privacy of the individual in relation to that information. One of the questions for consideration in this issues paper is therefore whether it is possible to design a legislative scheme for privacy that is "timeless" and can remain applicable despite developments in society and, in particular, in technology.

1.17 The Privacy Act 1993 came into force on 1 July 1993.[15] The Long Title to the Act describes it as:

> An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, ….

1.18 The Act is principally concerned with the protection of personal information about individuals (human beings, not companies). The Act provides a framework for regulating the collection, storage, use, and disclosure of personal information. It is mainly a data protection statute. It is principally concerned with information privacy – "control over access to private information or facts about ourselves"[16] – although some of its provisions give the Privacy Commissioner wider functions.

Key components of the Act

1.19 The key components of the Act are:

- what it applies to: personal information;
- who it applies to: agencies, both public and private;
- what it obliges agencies to do: comply with the privacy principles; and
- how those obligations are to be enforced: by the Privacy Commissioner and Human Rights Review Tribunal, not the courts.

15 Certain provisions did not become fully enforceable until some time later. In particular, the application of principle 11 to lists used for direct marketing was postponed until 1 July 1996 by section 9, and section 79 provided that breaches of most of the principles that occurred before 1 July 1996 could be the subject of a complaint to the Privacy Commissioner but could not be the subject of proceedings before the Complaints Review Tribunal (now the Human Rights Review Tribunal).

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

Personal information

1.20 The Act defines "personal information" as information about an identifiable individual.[17] "Individual" is defined as a natural person (human being), but not a deceased person.[18] However, information relating to a death that is maintained under the Births, Deaths, Marriages, and Relationships Registration Act 1995 is included in the definition of "personal information". The term "information" is not defined in the Act. Thus, "personal information" potentially includes any information about an individual, not just information that might be regarded as "private" or "personal", such as information about family, health, or other "sensitive" matters.

1.21 This can be contrasted with some overseas privacy legislation that categorises particular types or forms of information as especially private. For example, the Data Protection Act 1998 (UK) has special rules applying to "sensitive personal data", defined as personal data consisting of information pertaining to things such as the racial or ethnic origin of the subject, his or her political opinions or religious beliefs, his or her physical or mental health, or his or her sexual life.[19] The Privacy Act 1988 (Cth) likewise includes a definition of "sensitive information", which is also separately defined.[20]

Agency

1.22 The Act applies the privacy principles to personal information held by, and the information practices of, agencies. Like the definition of "personal information", the definition of "agency" is very wide.[21] It includes both public and private sector persons and bodies. An individual can be an agency for the purposes of the Act. But there are certain exclusions; a key exclusion is that of the news media in relation to their news activities.

Privacy principles

1.23 At the heart of the Act are 12 information privacy principles.[22] We refer to these throughout this issues paper simply as "privacy principles". The privacy principles set out when and how agencies may collect, store, use, and disclose personal information. In summary, the privacy principles are as follows (they are set out in full in Appendix A).

1.24 Principles 1 to 4 cover the collection of personal information.

1.25 *Principle 1:* An agency must not collect personal information unless it is for a lawful purpose connected with a function or activity of that agency, and the collection is necessary for that purpose.

---

17 Privacy Act 1993, s 2(1). The definition of "personal information" is discussed further in chapter 3.

18 Privacy Act 1993, s 2(1).

19 Data Protection Act 1988 (UK), s 2.

20 Privacy Act 1988 (Cth), s 6. See further the discussion in New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) para 7.50, about the difficulties of categorising particular types or forms of information as inherently private.

21 Privacy Act 1993, s 2(1).

22 The privacy principles are discussed in more detail in chapter 4.

1.26 *Principle 2:* An agency should generally collect personal information directly from the individual concerned.

1.27 *Principle 3:* Where an agency collects information directly from an individual, it must generally take reasonable steps to ensure that the individual is aware of:

- the fact that the information is being collected, and why it is being collected;
- who will receive the information;
- the identity of the agency that is collecting and will hold the information;
- the specific law (if any) governing the collection of the information and whether or not providing the information is voluntary or mandatory;
- the consequences (if any) if all or any of the information is not provided; and
- the individual's rights of access to the information and to have it corrected.

1.28 *Principle 4:* An agency must not collect personal information by unlawful means, or by means that are unfair or intrude to an unreasonable extent on the personal affairs of the individual concerned.

1.29 *Principle 5* is concerned with the storage and security of personal information. An agency that holds personal information must take steps to safeguard the information against loss; unauthorised access, use, modification, or disclosure; and other misuse.

1.30 Principles 6 and 7 are concerned with access to personal information by the person to whom it relates, and with correction of the information.

1.31 *Principle 6:* If an agency holds personal information in such a way that it can readily be retrieved, the person to whom the information relates is entitled to have confirmation of whether or not the agency holds the information, to have access to the information, and, if given access, to be told that he or she may request correction of the information. Agencies may refuse to give access to the information for a variety of reasons.

1.32 *Principle 7:* Individuals are entitled to request that personal information about them is corrected, and, if the information is not corrected, to request that there is attached to the information a statement of the correction sought but not made.

1.33 Principles 8 to 11 cover the use, retention, and disclosure of personal information.

1.34 *Principle 8:* An agency must not use personal information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

1.35 *Principle 9:* An agency must not keep personal information for longer than is required for the purpose for which the information may lawfully be used.

1.36 *Principle 10:* An agency that holds personal information obtained in connection with one purpose must not use it for another purpose. There are a number of situations in which this prohibition does not apply.

1.37 *Principle 11:* An agency must not disclose personal information except in certain specified circumstances.

1.38 *Principle 12* relates to unique identifiers, such as customer numbers. An agency must not assign a unique identifier to an individual unless this is necessary to enable the agency to carry out its functions efficiently, the identifier must be truly unique, and the identity of the individual must be clearly established. Unique identifiers assigned for one purpose do not have to be disclosed for another, unrelated, purpose.

Privacy Commissioner

1.39 The Act establishes the office of Privacy Commissioner as a Crown entity.[23] The Crown Entities Act 2004 provides that the Commissioner is an independent Crown entity,[24] which means that the Commissioner is generally independent of Government policy.

1.40 The functions of the Commissioner under the Act fall into four broad categories:[25]

- Compliance and enforcement, including the investigation of complaints about breaches of the privacy principles, a code of practice or the information matching provisions.
- Administration of the provisions of the Act, including the issuing of codes of practice, and the granting of specific exemptions from the privacy principles.
- Monitoring, research and policy, including undertaking periodic reviews of the Act, reviewing other legislation and policy that may affect individual privacy, and monitoring developments in technology.
- Education and publicity, including promoting, educating people about, and advising on the protection of information privacy and individual privacy generally, and inquiring into, and commenting and reporting on, privacy issues in general.

1.41 It is noteworthy that a number of the functions of the Privacy Commissioner are not restricted to matters relating to information privacy, but extend to privacy issues in general. These more general functions of the Privacy Commissioner were carried over from Part 5 of the Human Rights Commission Act 1977 (which was repealed by the Privacy Commissioner Act 1991).

1.42 In carrying out his or her functions, the Privacy Commissioner must, among other things, have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of the free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.[26]

---

23 Privacy Act 1993, s 12.

24 Crown Entities Act 2004, sch 1, pt 3.

25 The role and functions of the Commissioner are discussed further in chapter 6.

26 Privacy Act 1997, s 14.

Complaints

1.43 A central feature of the New Zealand approach to compliance with the Act is the provision of a low-cost and non-judicial mechanism for individuals to challenge the actions of agencies in dealing with their information and obtain redress in appropriate cases.[27] With one exception, the privacy principles do not confer legal rights that are enforceable in a court of law.[28] That exception is the right of an individual to obtain access to personal information about him or her that is held by a public sector agency.

1.44 Complaints under the Act are made initially to the Privacy Commissioner. The Commissioner's functions in relation to complaints are to investigate, act as a conciliator, and take such further action as is contemplated by Part 8 of the Act (that is, investigation and settlement of complaints, and action in the Human Rights Review Tribunal).[29] Upon receiving a complaint, the Commissioner may investigate the complaint or, in certain circumstances, decide to take no action.[30]

1.45 If, after investigating a complaint, the Commissioner is of the opinion that it has substance, the Commissioner must use his or her best endeavours to secure a settlement between the parties and, if appropriate, a satisfactory assurance that there will not be a repetition of the cause of the complaint.[31] If the attempt to reach a settlement is unsuccessful, the Commissioner may refer the matter to the Director of Human Rights Proceedings for the purpose of deciding whether proceedings should be instituted in the Human Rights Review Tribunal against the agency complained about.[32] If the Director decides to institute proceedings, the Director acts as the plaintiff, rather than appearing for the aggrieved individual.[33] In addition, the aggrieved individual may himself or herself bring proceedings in some circumstances.[34]

1.46 If the Tribunal is satisfied, on the balance of probabilities, that any action of the defendant is an interference with the privacy of an individual, it may grant one or more remedies, which are detailed in chapter 8.

1.47 An appeal lies to the High Court against a decision of the Human Rights Review Tribunal,[35] and there is a further right of appeal to the Court of Appeal on a question of law.[36]

---

27 For further discussion of the complaints provisions of the Act see chapter 8.

28 Privacy Act 1993, s 11. Note section 28 of the Wanganui Computer Centre Act 1976 (repealed), which provided a right of action against the Crown for damages in respect of loss or damage suffered as a consequence of the release of certain information from the Wanganui Computer Centre system.

29 Privacy Act 1993, s 69.

30 Privacy Act 1993, ss 70–71.

31 Privacy Act, s 77(1)(a).

32 Privacy Act 1993, s 77(2).

33 Privacy Act 1993, s 82.

34 Privacy Act 1993, s 83.

35 Human Rights Act 1993, s 123 (which applies by dint of Privacy Act 1993, s 89).

36 Human Rights Act 1993, s 124 (which applies by dint of Privacy Act 1993, s 89).

Offences

1.48 The Privacy Act contains no offences for a breach of any of the provisions of the Act relating to privacy of information, although it does create a small number of offences which relate mainly to impeding the legitimate activities of the Privacy Commissioner.[37]

Exemptions from the Act

1.49 Exemptions from the Act include the following:[38]

- Some entities are excluded from the definition of "agency", effectively exempting them from the coverage of the privacy principles.
- Certain privacy principles are overridden by other legislation that authorises or requires personal information to be made available, or that prohibits, restricts, or regulates the availability of personal information. In addition, an action that is authorised or required by law is not a breach of principles 1 to 5, 7 to 10, and 12.[39]
- The privacy principles do not apply in respect of the collection or holding of personal information by an individual, if the information is collected or held solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs.[40]
- Privacy principles 1 to 5 and 8 to 11 do not apply in relation to information collected, obtained, held, used, or disclosed by, or disclosed to, the New Zealand Security Intelligence Service or the Government Communications Security Bureau.[41]
- The Privacy Commissioner is empowered to authorise an agency to collect, use, or disclose personal information, even though it would be in breach of principles 2, 10, or 11, if the Commissioner is satisfied of certain matters.[42]

1.50 Some of the privacy principles themselves also contain detailed exceptions from their application. Part 11 and Schedule 5 of the Act specifically authorise certain public sector agencies to have access to "law enforcement information" held by other agencies.

1.51 If an agency wants to claim that an exception applies to it, the onus is on that agency to prove that the exception applies.[43]

37 Privacy Act 1993, s 127.

38 For further discussion see chapter 5.

39 Privacy Act 1993, s 7. For further discussion see chapter 11.

40 Privacy Act 1993, s 56.

41 Privacy Act 1993, s 57.

42 Privacy Act 1993, s 54.

43 Privacy Act 1993, s 87.

Codes of Practice

1.52 Part 6 of the Act authorises the Privacy Commissioner to issue codes of practice in relation to information of certain kinds, or in respect of certain kinds of agency, activity, industry, profession, or calling. A code of practice may modify the application of any one or more of the privacy principles, or prescribe how any one or more of the principles are to be applied or complied with. A code may prescribe standards that are more or less stringent than the relevant principle, or exempt actions from a principle unconditionally or subject to conditions.[44]

1.53 The following codes of practice have been issued under the Act and are currently in force:

- Health Information Privacy Code 1994;
- Superannuation Schemes Unique Identifier Code 1995;
- Justice Sector Unique Identifier Code 1998;
- Telecommunications Information Privacy Code 2003; and
- Credit Reporting Privacy Code 2004.

Two codes have been revoked.

1.54 Codes of practice are a form of delegated legislation, but are issued by the Commissioner and do not go through the normal Cabinet approval process that applies to ordinary statutory regulations. However, codes must be presented to the House of Representatives after they are made, and are subject to disallowance under the Regulations (Disallowance) Act 1989.[45]

Public registers

1.55 Part 7 of the Act sets out four public register privacy principles that apply to public registers. Public registers were the subject of stage 2 of the Law Commission's review of the law of privacy,[46] and are not dealt with in this issues paper.[47] The Law Commission recommended that its recommendations on public registers should be considered by the Government once stage 4 of the Law Commission's privacy Review is completed, so that proper consideration can be given to all the privacy issues arising out of the Review in a coordinated manner.

Information matching

1.56 Part 10 and Schedules 3 and 4 of the Act relate to information matching by public sector agencies. Information matching essentially involves the comparison of personal information from one source against personal information from another source, for the purpose of producing or verifying information about an

44 Codes are discussed further in chapter 7.

45 Privacy Act 1993, s 50.

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

47 See also John Edwards "Public Registers and Privacy" [2007] NZLJ 146.

identifiable individual. A common application of information matching is to detect fraud in the delivery and receipt of social assistance programmes such as social welfare benefits and student allowances.

1.57 The Act controls information matching by requiring that it be authorised by statute, that information matching programmes carried out by agencies be done pursuant to information matching agreements that comply with certain rules, and that certain procedural safeguards are followed before action is taken in reliance on the results of a matching programme.

PRECURSOR LEGISLATION OR LEGISLATIVE ATTEMPTS TO DEAL WITH PRIVACY

Privacy initiatives in the 1970s

1.58 The 1970s saw a number of attempts to enact legislation to deal with aspects of privacy. The Preservation of Privacy Bill 1972 and the Right to Confidentiality Bill 1974 were private members' bills which did not proceed. The first was concerned with computer privacy, the second with doctor and social worker confidentiality. In 1975 the Bill which became the Wanganui Computer Centre Act 1976 was introduced. It was accompanied by the Listening Devices Bill 1975 and the Privacy Commissioner Bill 1975. These latter two Bills did not proceed, but some of the provisions of the first later found their way into a new part 9A of the Crimes Act 1961 relating to crimes against personal privacy. The second, which would have created a Privacy Commissioner with an oversight and advisory role, was effectively a precursor to Part 5 of the Human Rights Commission Act 1977.

Wanganui Computer Centre Act 1976

1.59 The Wanganui Computer Centre Act 1976 made provision for the establishment and operation of the Wanganui Computer Centre, which was to store, process, and retrieve information in order to aid the Police, Department of Justice, and the Ministry of Transport in their law enforcement functions.

1.60 The Act specified what information could be stored on the computer system, and which types of information could be retrieved by which departments.[48] Gaining or attempting to gain unauthorised access to the system was an offence.[49]

1.61 A Wanganui Computer Centre Policy Committee and a Wanganui Computer Centre Privacy Commissioner were established.[50] The function of the policy committee was to determine the policy of the computer centre relating to the privacy, and the protection of the rights, of the individual insofar as these were affected by the operation of the computer system, and its specific powers included determining how long records of requests for information from the computer system should be kept. The functions of the Privacy Commissioner included the receipt and granting of requests from individuals for a copy of the information about them stored on the computer system, and the investigation of complaints from individuals about information wrongly recorded on the computer system.[51]

48 Wanganui Computer Centre Act 1976, s 4.

49 Wanganui Computer Centre Act 1976, s 29.

50 Wanganui Computer Centre Act 1976, s 5.

51 Wanganui Computer Centre Act 1976, s 9.

1.62 The Act created a right of action against the Crown for the recovery of damages in respect of loss or damage as a consequence of incorrect or unauthorised information about that person having been made available to any person by the computer system, or authorised information about that person having been made available by the computer system to any person not authorised to receive it.[52]

Human Rights Commission Act 1977

1.63 The Human Rights Commission Bill was introduced on 9 December 1976. On introduction the Minister in charge of the Bill described the effect of Part 5 of the Bill as follows:[53]

> Part V of the Bill gives the commission general powers to inquire into matters affecting privacy and to make reports to the Prime Minister. There will, however, be no power to investigate individual complaints. Rather, the commission will have the role of advising successive Governments on how privacy may best be protected.

1.64 During the second reading, the Acting Minister of Justice commented that:[54]

> The purpose of clause 58 [later section 67] is to assist the Government to take such action as may from time to time be necessary to give better protection to individual privacy. The commission should, in due course, become a repository of much useful information on privacy matters, and should be able to pinpoint problem areas for future action.

Information Privacy Bill 1991

1.65 The Information Privacy Bill was introduced as a private member's Bill on 5 June 1991 by the Hon Peter Dunne.[55] It was read a first time and referred to the Justice and Law Reform Committee.

1.66 The Bill was in many respects similar to the Privacy of Information Bill introduced by the Government later in 1991. It covered the public sector, companies, and incorporated societies, provided for a set of privacy principles, set up a Privacy Commissioner and a complaints procedure, and dealt with information matching.

1.67 At the time of the introduction of the Bill, the Government indicated that it intended to introduce its own privacy legislation within a few months.

1.68 The Bill was essentially superseded by the Privacy of Information Bill introduced by the National Government in August 1991.

52 Wanganui Computer Centre Act 1976, s 29.

53 (9 December 1976) 408 NZPD 4688.

54 (23 August 1977) 413 NZPD 2393.

55 (5 June 1991) 515 NZPD 2154.

Background

1.69 The Labour Government indicated in 1987 that its three-year legislative programme included the introduction of legislation relating to data protection and issues of personal privacy. This was announced by the Rt Hon Geoffrey Palmer, Deputy Prime Minister and Minister of Justice, in the Address in Reply debate on 6 October 1987. He said:[56]

> Other important legislation that will be introduced during the 3-year legislative period involves the right to privacy. New Zealand is in considerable difficulty in relation to the inadequate nature of its data protection law, and issues of personal privacy. The Government is working on those matters, and Bills that relate to them will be introduced into Parliament within the 3-year legislative programme.

1.70 In 1987, the Information Authority established under the Official Information Act 1982 issued a report recommending that a set of privacy principles covering the collection and use of personal information by departments and organisations be included in Part 4 of the Official Information Act 1982.[57]

1.71 An options paper on data privacy, written by Tim McBride, was released for public comment and submissions in December 1987.[58] However, it was not until 1991 that privacy legislation was actually introduced.

Privacy of Information Bill 1991

1.72 On 5 August 1991, the Privacy of Information Bill was introduced into the House of Representatives and read a first time.[59] The Bill was referred to the Justice and Law Reform Committee.

1.73 The legislation had two purposes: to authorise greater information sharing between government agencies to detect fraud and abuse of the social welfare system, and to protect individual privacy by imposing controls on information sharing.

1.74 The Minister in charge of the Bill, the Hon DAM Graham, on the first reading on the Bill, linked those two objectives as follows:[60]

> It follows that if there is to be any extension of the right of Government to use information relating to individual members of the public, then there should be a mechanism in place to ensure that there is proper parliamentary authority for that use of information, and adequate safeguards against the abuse of that power. This Bill provides that necessary statutory authority and enacts the safeguards.

1.75 The Minister also referred to the international context. He referred to two international documents as being of particular relevance to New Zealand and the issue of privacy. These were the International Covenant on Civil and Political Rights adopted by the United Nations in 1966 (ratified by New Zealand in 1978),

56 (6 October 1987) 483 NZPD 401.

57 Information Authority *Personal Information and the Official Information Act: Recommendations for Reform* (Wellington, 1987).

58 Tim McBride *Data Privacy: An Options Paper* (Government Printer, Wellington, 1987).

59 (5 August 1991) 518 NZPD 3848.

60 (5 August 1991) 518 NZPD 3848.

and the Organisation for Economic Co-operation and Development Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data, recommended by the OECD in 1980. He indicated that the Bill was being introduced in recognition of the need to harmonise New Zealand data privacy law with the international community.[61]

1.76 In addition, the Minister indicated that the Bill was necessary even if comity with international privacy law were not a consideration. He referred to the fact that, in New Zealand, there was little control over the exchange of information. Some statutory provisions imposed prohibitions on the dissemination of information by Government departments, but they were few and far between and did not provide a holistic approach. There were even fewer laws in New Zealand providing a regime to promote information privacy in the private sector.

1.77 The Opposition did not oppose the introduction of the Bill.

1.78 The Bill as introduced had a commencement date of 1 November 1991, although certain provisions (such as those providing for complaints to the Privacy Commissioner) were to be brought into force later by Order in Council. The Minister of Justice acknowledged the tight timeframe that this imposed on the select committee to consider the Bill and report it back. He indicated that one option would be for the provisions of the Bill authorising the exchange of information between government departments (Part 12) to be split off from the Bill and reported back and enacted separately.

Privacy Commissioner Act 1991

1.79 In the event, the Bill was divided by the select committee. The Privacy Commissioner Bill, comprising the parts relating to the establishment, functions, and powers of the Privacy Commissioner, information matching, and the amendments to other legislation relating to authorised information matching, was split off and reported back on 21 November 1991.

1.80 The Bill was then enacted as the Privacy Commissioner Act 1991 (assented to on 18 December 1991), along with some amendments authorising information matching by certain government departments.

1.81 On the report back of the Privacy Commissioner Bill, the chair of the Justice and Law Reform Committee, Mr Munro, indicated that the select committee had not been able, in the time available, to give the whole Bill the full scrutiny it required.[62]

1.82 The select committee therefore recommended a two-stage approach. The immediate issue of combating fraud and abuse of the social welfare system should be addressed by enacting the amendments authorising information matching, along with certain safeguards. The office of Privacy Commissioner should also be established immediately as one of those safeguards, with the role of overseeing and monitoring information matching. The second stage would be for the select

61 (5 August 1991) 518 NZPD 3849.

62 (21 November 1991) 520 NZPD 5512.

committee, with the assistance of the Privacy Commissioner, to continue its examination of the Bill, consider the options available to deal with the wider privacy issues raised by the Bill, and report back to the House.

1.83 In April 1992, Bruce Slane was appointed as the first Privacy Commissioner under the Privacy Commissioner Act 1991.

Privacy of Information Bill reported back

1.84 The Bill was reported back from the Justice and Law Reform Committee on 18 March 1993.[63] The following are the key changes recommended by the select committee.

Name of Bill

1.85 The select committee recommended that the name of the Bill be changed from "Privacy of Information Bill" to "Privacy Bill". The select committee considered that, although the Bill related principally to information privacy, the Privacy Commissioner did have a wider role in relation to matters of privacy.

Definition of agency

1.86 The select committee recommended that the following be excluded from the coverage of the Bill:

- Members of Parliament in their official capacity, and the Parliamentary Service (except in relation to personal information about employees or former employees);
- courts, in relation to their judicial functions; and
- the news media, in relation to their news activities.

Privacy principles

1.87 The Bill as introduced contained 14 privacy principles. The select committee recommended that two be omitted: the requirement that agencies maintain a register of personal information held by them, and the requirement for public sector agencies to provide reasons for decisions or recommendations made about individuals.

1.88 A new privacy principle relating to unique identifiers was recommended. This was to replace the unique identifier provisions of the Bill as originally introduced, which empowered the making of regulations governing the creation and use of unique identifiers.

1.89 The select committee recommended that the privacy principle that limited the disclosure of personal information should not apply to the activities of direct marketers until three years after the Bill came into force.

1.90 The other recommendations essentially related to the clarification, refinement, and reordering of the original privacy principles.

63 (18 March 1993) 533 NZPD 14132.

Charging for access to and correction of personal information

1.91 The Bill as introduced did not allow public or private sector agencies to impose a charge in relation to access requests by individuals. The select committee considered that this prohibition was not consistent with the commercial imperatives of private sector agencies. It therefore recommended that they be able to impose a reasonable charge for access requests.

Exemptions from privacy principles

1.92 The Bill as introduced empowered the Equal Opportunities Tribunal (which was to be renamed the Complaints Review Tribunal) to grant exemptions from all or any of the privacy principles. The select committee recommended that this power be replaced with two alternative procedures:

- provision for the Privacy Commissioner to issue codes of practice modifying the application of one or more of the privacy principles or prescribing how they were to be applied; and
- provision for the Privacy Commissioner to authorise the collection, use, or disclosure of personal information, despite this being in breach of the relevant privacy principles, where the Commissioner is satisfied that there is an outweighing public interest or a clear and outweighing benefit to the individual concerned.

Public registers

1.93 As introduced, the Bill contained no special provision in respect of personal information on public registers. The select committee recommended that the Bill be amended by inserting a new Part establishing a special regime applying to public registers. The new Part included a set of public register privacy principles.

Complaints relating to interference with privacy

1.94 The Bill as introduced provided that an action was an interference with the privacy of an individual if, among other things, the action was considered by the Privacy Commissioner to be contrary to law, unreasonable, unjust, oppressive, improperly discriminatory, or based on a mistake of law or fact; or if a discretionary power had been exercised for an improper purpose, or on irrelevant grounds, or on the taking into account of irrelevant considerations. This test was imported from the Ombudsmen Act 1975, and had very much a legal flavour.

1.95 The select committee recommended that this test be replaced with one that focused more generally on the impact on the individuals whose privacy was infringed. It recommended that the test be whether or not the action complained about has caused, or may cause, loss, detriment, damage, or injury to the individual or has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual.

Information matching

1.96 In the Bill as introduced, the privacy principle that restricted when personal information obtained for one purpose could be used for another purpose allowed the information to be used for an information matching programme, if authorised by the Privacy Commissioner. The provision applied to both the public and the private sectors.

1.97 The select committee recommended that the provisions of the Bill relating to information matching effectively be turned into a special regime for public sector agencies only, and only in the case of specified agencies and specified information matching programmes authorised by statute. The Privacy Commissioner would no longer authorise information matching programmes, but would monitor authorised programmes and examine legislative proposals to establish new information matching programmes.

Amendments to Health Act 1956 relating to disclosure of health information

1.98 The Bill as introduced proposed to simply repeal sections 22B to 22F of the Health Act 1956, which at the time related to a health computer system under the control of the Director-General of Health, and imposed controls and protections with respect to the collection and disclosure of personal information by the then Department of Health.

1.99 By the time the Bill was considered by the Justice and Law Reform Committee in late 1992 and early 1993, the Health and Disability Services Bill had been introduced. That Bill implemented the then Government's health reforms, including the creation of regional health authorities, Crown Health Enterprises, and a Public Health Commission in substitution for area health boards. On the report back on that Bill, the chair of the Social Services Committee indicated that the provisions of the Health Act 1956 relating to the privacy of health information needed to be rewritten in the light of the new health structure.

1.100 The Privacy of Information Bill as reported back therefore included new amendments to the Health Act 1956.

Second reading

1.101 The Bill was given its second reading on 20 April 1993.[64]

1.102 Of particular note are the comments of the Minister in charge of the Bill, the Hon DAM Graham, on exclusions from the coverage of the Bill. He noted the exclusion from the Bill of Members of Parliament and Parliamentary agencies, the news media, and intelligence agencies. He stated as follows:[65]

> There are also exemptions and partial exemptions that are suitable now but that it is intended will be re-examined as time goes on. I am referring to the provisions on members of Parliament, the Parliamentary Service Commission, the Parliamentary Service, the news media, and the intelligence agencies. Members of Parliament and supporting services are concerned with the passing of legislation, and this legislative

64 (20 April 1993) 534 NZPD 14721.

65 (20 April 1993) 534 NZPD 14721.

> function is excluded in jurisdictions similar to ours. The news media are also excluded in many, but not all, jurisdictions. The freedom of the press is essential in any democracy, and more work is required to ensure that that freedom is not jeopardised in relation to privacy principles. The Bill gives power to the Privacy Commissioner to review the Act after 3 years, then at intervals of 5 years. The consequence of these reviews should be gradually to bring within the scope of the law those bodies I have listed, given the importance to them of the proper handling of personal information.

Committee of the whole House and third reading

1.103 The committee of the whole House stage and the third reading of the Bill (and the Bills into which it was divided) were both completed on 5 May 1993. The third reading was agreed to unanimously by the Government and the Opposition.[66] Members who spoke on the third reading considered that Parliament had produced a workable piece of legislation that struck the right balance between the protection of the rights of individuals to privacy with respect to their personal information, and other interests that compete with privacy. The fact that the Bill was passed unanimously no doubt reflects the fact that, as can be seen from the history of privacy legislation in New Zealand outlined above, both major political parties of the time recognised that New Zealand's data protection law was inadequate and that new safeguards for personal privacy needed to be enacted.

1.104 The Bill received the Royal assent on 17 May 1993.

THE INTERNATIONAL CONTEXT

1.105 In *Privacy: Concepts and Issues*, we highlighted the vital importance of the international dimension of privacy.[67] We do not repeat the detail of that discussion here, and chapter 14 examines the issue of trans-border data flows in detail. Here we simply note the fact that the Privacy Act does not exist in jurisdictional isolation, but takes its place as part of the international web of national laws and regional and international conventions and treaties. This fact is an important consideration in reviewing the Act. To what extent does it stand up alongside similar legislation in other jurisdictions, and in relation to New Zealand's international obligations? To what extent is compatibility with the privacy laws of other jurisdictions, particularly Australia, important?

1.106 Section 14 of the Act, which sets out certain matters to which the Privacy Commissioner is to have regard in exercising or performing his or her functions and powers, requires the Commissioner to:

- take account of international obligations accepted by New Zealand, including those concerning the international technology of communications; and
- consider any developing general international guidelines relevant to the better protection of individual privacy.

66 (5 May 1993) 535 NZPD 15209.

67 New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) 20–21 and Chapter 7.

1.107 We noted in *Privacy: Concepts and Issues* that "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."[68] There is, therefore, no overall standard against which to measure the Act. However, the following international frameworks and instruments are relevant to our review of the Privacy Act:

- Article 17 of the International Covenant on Civil and Political Rights, which provides for a right to be free from arbitrary or unlawful interference with privacy.[69]
- The 1980 Recommendation of the Council of the OECD Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The Long Title to the Privacy Act specifically states that the Act is to promote and protect individual privacy in general accordance with the OECD Guidelines.
- The APEC Privacy Framework, endorsed by the Asia-Pacific Economic Cooperation (APEC) group of countries in 2005.[70]
- The European Union Directive on the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of such Data.[71] The amendments to the Privacy Act proposed in the Privacy (Cross-border Information) Amendment Bill are intended in part to address issues of the adequacy of New Zealand law with respect to this Directive.

1.108 In addition, the Closer Economic Relationship (CER) agreement between New Zealand and Australia has resulted in free trade between the two countries in goods and services, and "both countries have moved progressively towards much deeper cooperation in policies, laws and regulatory regimes through processes of coordination, mutual recognition and harmonisation".[72] With many companies doing business on both sides of the Tasman, and the common labour market between the two countries, the harmonisation of information privacy laws between the two countries is a real issue. New Zealand is also entering into a growing number of free trade agreements with other states, which might give rise to a similar issue.

---

68 New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) para 7.23.

69 New Zealand is required to submit regular reports on the measures that it has adopted which give effect to the rights in the Covenant and on progress made in the enjoyment of those rights. The latest report was presented in December 2007: *International Covenant on Civil and Political Rights: Fifth Periodic Report of the Government of New Zealand, 21 December 2007*. Compliance with article 17 of the Covenant is dealt with at paragraphs 265 to 287.

70 Asia-Pacific Economic Cooperation "APEC Privacy Framework" (2004/AMM/0114rev1, 16th APEC Ministerial Meeting, Santiago, 17–18 November 2004).

71 EC 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.

72 Ministry of Foreign Affairs and Trade *Trade Matters: Trans-Tasman Closer Economic Relations: What is CER?* www.mfat.govt.nz/Media-and-publications/Publications/Trade-matters/0-cer.php (accessed 14 December 2009).

OUR APPROACH IN THIS REVIEW

1.109 In reviewing the Privacy Act, we must keep in mind the need to ensure that:

- the Act remains broadly consistent with relevant international privacy instruments, and with the information privacy laws of our trading partners;
- the Act continues to be relevant and effective as technological developments affect the ways in which information can be collected, stored and used;
- lessons are learned from the practical experience of working with the Act, including any difficulties in applying the Act that have emerged; and
- privacy is balanced with other rights and interests, including freedom of information; public health, safety and welfare; law enforcement; and effectiveness and efficiency of government and business operations.

Chapter 2

Scope, approach, and structure of the Act

2.1 This chapter examines the current scope, approach, and structure of the Act, and whether any changes are required. The matters covered in this chapter are:

- a description of the Act's current scope (a data protection statute more than a general privacy statute), approach (open-textured and principles-based, rather than rules-based), and structure (including its name), and whether any changes are required to these aspects of the Act;
- how the Act attempts to balance privacy with competing or countervailing interests, and whether or not the balance struck is appropriate;
- the costs of complying with the Act, and whether or not there are ways in which compliance can be made easier and less costly without compromising the Act's objectives;
- common perceptions and misunderstandings about the Act, and whether or not these can be remedied; and
- the various kinds of instruments and advice issued by the Privacy Commissioner.

CURRENT SCOPE AND APPROACH OF THE ACT

What the Act covers

2.2 Despite its general title, the Act is more about information privacy than about other aspects of privacy. The Act provides a framework regulating the collection, storage, use and disclosure of personal information – that is, information about individuals. The Act is principally a data protection statute, although some of the functions of the Privacy Commissioner extend more widely.

2.3 Nevertheless, within those parameters, the coverage of the Act is very broad. The Privacy Commissioner made the following observation in *Necessary and Desirable*:[73]

> A principal feature of the Act is its broad coverage:
>
> - it covers all "agencies" whether in the public or private sectors; and
> - it applies to all "personal information".

73 *Necessary and Desirable* 4.

> Broad coverage gives confidence that the information privacy principles apply in nearly all circumstances. The greater the inroads into the types of agencies or information covered, the greater the possibility of privacy being left unprotected. The broad coverage of the Act is also the surest guarantee that our law will be considered to offer "adequate protection" in respect of the tests established in the EU Directive on Data Protection. It also avoids compliance costs, creates certainty, avoids demarcation disputes or gaps between codes of practice about coverage.

2.4 There are some agencies that are excluded from the Act's coverage (such as the news media), and some kinds of personal information are also excluded (such as personal information held by an individual solely or principally in connection with his or her personal, family, or household affairs). We examine these exclusions and exemptions in detail in chapter 5.

2.5 While the core provisions of the Act relate to information privacy, the Privacy Commissioner has some statutory functions that extend wider than simply information privacy. These functions, which are contained in section 13(1), are set out in full in chapter 6. The Privacy Commissioner also has functions under a number of other enactments. In chapter 6 we consider the Commissioner's functions more fully.

Open texture vs rule-based

2.6 The Act regulates the collection, storage, use, and disclosure of personal information through a set of privacy principles, and provides for their enforcement through the Privacy Commissioner and the Human Rights Review Tribunal. A key feature of the Act is that it is not rules-based. It is principles-based and open-textured, and regulates in a rather light-handed way. The open-textured nature of the Act means that judgement is required in its application since it does not set out detailed steps for agencies to follow or provide a checklist for compliance. The privacy principles must be applied and assessed in relation to each individual set of facts as they arise.

2.7 The flexibility of the Act is seen as one of its strengths. The Privacy Commissioner has described the approach of the Act as "outcomes-oriented".[74] The Act prescribes certain standards, but agencies have a great deal of flexibility in the ways in which they may comply with them. The compliance mechanisms available under the Act reinforce this flexibility. Although sanctions against non-compliance with the principles are available in proceedings before the Human Rights Review Tribunal, the focus of the Privacy Commissioner's complaints investigation process is on working through the issues with the parties involved and securing a settlement. In appropriate cases, this may also involve an assurance that the action complained about will not be repeated.

2.8 The flexibility of the Act is supplemented by the power of the Privacy Commissioner to promulgate codes of practice. In this way, the specific needs and circumstances of particular agencies, groups of agencies, businesses or industries can be accommodated through the ability of a code of practice to modify the application of the privacy principles or prescribe how they are to be applied or complied with. We examine codes of practice in more detail in chapter

74 *Necessary and Desirable* 7.

7. Further, section 54 of the Act authorises the Privacy Commissioner to grant specific authorisations to collect, use, or disclose personal information, even though this would otherwise be in breach of a privacy principle. There are also some quite detailed rules about information matching in Part 10: these are discussed in chapter 9.

2.9 The overall approach adopted in the New Zealand Privacy Act is similar in this respect to the Australian Privacy Act 1988. It is quite a different approach from that adopted in the United Kingdom and Europe. There, registration systems are the norm. The UK Data Protection Act 1998 has a set of data protection principles with which all "data controllers" (persons who process personal data) must comply, but it also requires data controllers to be registered with the Information Commissioner. Processing personal data without registration is an offence.

2.10 The European regulatory framework relating to data privacy has been summarised as follows:[75]

> The European regulatory framework thus embraces a number of principles with regard to personal data processing, such as the proportionality and transparency of the processing, and the limitation of the processing to specific purposes which are agreed (or at least clearly communicated) between the data controller and the data subject. The respect of these principles is possible through the definition of standard roles (most notably the data controller, processor and data subject), each of whom has specific rights and obligations under this legal framework.
>
> This framework however takes a very static and formal approach to data processing, and as a result struggles to cope with the new privacy challenges presented in the information society. Its approach is largely based on a number of tacit assumptions which were substantially valid a decade ago, but which are much harder to apply in a society where personal data has become a fluid and mutable resource that can change form, scope and ownership overnight.

2.11 In undertaking a review of the Privacy Act in 1998, the then Privacy Commissioner did not consider that a change to the current principles-based approach of the Act was warranted.[76]

2.12 The Australian Law Reform Commission's (ALRC) report concludes that "principles-based" regulation should remain the primary method of regulating information privacy in Australia, supplemented with more specific rules (regulations or industry codes) to accommodate the particular needs and circumstances of different industries, and guidance, advice, and education provided by the Privacy Commissioner.[77] This conclusion is based on what the ALRC identifies as the following advantages of a principles-based approach:[78]

- Rather than being unduly prescriptive, it provides an "overarching framework that guides and assists regulated agencies to develop an appreciation of the

75 Rand Corporation *Review of EU Data Protection Directive: Inception Report* (Cambridge, 2008) para 2.1.3.

76 *Necessary and Desirable* para 2.1.11.

77 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 111.

78 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 4.4–4.18.

core goals of the regulatory scheme". In this way it promotes compliance with the spirit of the law, rather than a focus on finding and exploiting loopholes in the law and a consequent loss of focus on the regulatory objectives.

- It facilitates compliance by allowing regulated agencies to develop policies or other mechanisms that both comply with the rule and meet the agency's needs.
- The emphasis on outcomes rather than prescriptive rules allows regulated agencies "to work towards effective implementation of the principles within their own organisational context", thereby minimising the need for regulatory intervention and red tape.
- It facilitates "regulatory flexibility through the statement of general principles that can be applied to new and changing situations" (durability).

2.13 Professor Julia Black has summarised the arguments in favour of principles-based regulation as follows:[79]

> For firms, principles-based regulation can provide flexibility, facilitate innovation and so enhance competitiveness. Principles based regulation can be beneficial for regulators too: it can provide them with flexibility, facilitate regulatory innovation in the methods of supervision adopted; enable the regulatory regime to have some durability in a rapidly changing market environment; and enhance regulatory competitiveness. Other stakeholders can benefit from the improved conduct of firms as they focus more on improving substantive compliance and achieving outcomes and less on simply following procedures, box-ticking or on working out how to avoid the rule in substance whilst complying with its form: 'creative compliance'.

2.14 A further perceived advantage is that principles are more accessible to those to whom they apply than "a bewildering mass of detailed requirements".[80]

2.15 The arguments in favour of a rules-based approach are essentially the flip-side of the criticisms of the principles-based approach. It is said that rules provide greater clarity, certainty, and predictability for those who are regulated, so that they know what they have to do to comply with the requirements and what constitutes a minimum standard of compliance. They are also said to be fairer, because the same rules apply to everyone, and a strict system of rules, particularly those of the "bright line" variety, is said to facilitate their enforceability. It is harder for those regulated to circumvent rules that are clear and precise, and consequently easier for regulatory authorities to establish and prosecute a breach of them.[81]

79 Julia Black "Forms and Paradoxes of Principles Based Regulation" (LSE Law, Society and Economy Working Paper, London School of Economics and Political Science, 2008) 3.

80 Julia Black "Forms and Paradoxes of Principles Based Regulation" (LSE Law, Society and Economy Working Paper, London School of Economics and Political Science, 2008) 10.

81 See further O Krackhardt "New Rules for Corporate Governance in the United States and Germany – A Model for New Zealand" (2005) 36 VUWLR 319, 330–333.

2.16 Of course the differences between principles-based and rules-based approaches are never cleanly and sharply defined. As concepts, they constitute high-level generalisations of what are numerous points on a spectrum of approaches, they can take different forms,[82] and in terms of their practical application there is a blurring of approach through the natural human tendency to "'round off' the hard corners of rules and 'sharpen' the soft edges of principles."[83]

2.17 Neither is it necessarily a case of choosing one approach or the other. There may be room within any regulatory scheme for a combination of approaches – a hybrid system. As pointed about above, the Privacy Act itself combines the principles-based approach with provision for more detailed rules prescribed in codes of practice. In addition, some of the exceptions to the principles provided for in the Act are specific and narrowly focussed. Indeed, the combination of general principle and specific exceptions is a feature of the New Zealand legislation. Detailed rules may also exist outside of, and override, the principles-based scheme in certain circumstances. Thus, the Privacy Act gives way to other legislation that, for example, authorises or requires particular personal information to be made available, or prohibits or restricts the availability of particular personal information (section 7).

2.18 The ALRC gives three reasons for adopting principles-based regulation to guide it in developing tools to regulate privacy in Australia.[84] These are:

- Flexibility in comparison to rules: "Being high-level, technology-neutral, and generally non-prescriptive, principles are capable of application to all agencies and organisations subject to the *Privacy Act*, and to the myriad of ways personal information is handled in Australia."
- Future-proofing: "Principles allow for a greater degree of 'future-proofing' and enable the regime to respond to new issues as they arise without having to create new rules."
- Stakeholder support: "the ALRC recognises the considerable support by stakeholders for retaining principles as the primary regulatory method in the *Privacy Act*."

2.19 Having said that, the ALRC goes on to state that it does not recommend a pure form of principles-based regulation for privacy. Recognising the limitations inherent in principles-based regulation set out above, the ALRC describes its approach as pragmatic, and its model as a hybrid system of principles and rules. "While principles-based regulation forms the foundation of the ALRC's approach, the model allows for these principles to be supplemented by more specific rules in regulations or other legislative instruments, to accommodate different industries or different policy considerations."[85]

---

82 For a fuller discussion, see Julia Black "Forms and Paradoxes of Principles Based Regulation" (LSE Law, Society and Economy Working Paper, London School of Economics and Political Science, 2008) 12–24.

83 Julia Black "Forms and Paradoxes of Principles Based Regulation" (LSE Law, Society and Economy Working Paper, London School of Economics and Political Science, 2008) 12, citing F Schauer "The Tyranny of Choice and the Rulification of Standards" (2005) 14 J Contemp Legal Issues 803.

84 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ARLC R108, Sydney, 2008) paras 4.27–4.30.

85 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ARLC R108, Sydney, 2008) para 4.35.

2.20 The Law Commission's own preliminary conclusion is that, for those same reasons of flexibility and future-proofing, the New Zealand Privacy Act should continue to be based on the principles-based regulatory approach. We note that in *Privacy: Concepts and Issues*,[86] we raised the question of whether domestic privacy 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. In our view, the open-textured nature of the Privacy Act, and in particular the balancing exercise required under section 14 which specifically requires the Privacy Commissioner to consider New Zealand's international obligations and any developing general international guidelines relevant to the better protection of individual privacy, go a long way towards what we consider to be desirable flexibility in this area.

2.21 In addition, the huge changes in technology, particularly the emergence and importance of the internet, since the Privacy Act was passed, show that an open-textured and flexible approach to privacy is warranted and indeed essential. It is hard to see how any other approach can effectively future-proof the Act (so far as that is possible) in the face of further developments and challenges in this sphere.

2.22 Having stated this as its preliminary conclusion, the Law Commission is nevertheless keen to hear from submitters on this issue. We deal with other aspects of the existing "hybrid model", the role of codes of practice and the relationship between the Privacy Act and personal information-related rules in other legislation, and the impact of technology, later in this issues paper.

Q1 We believe that the "principles-based", open-textured approach to information privacy regulation in New Zealand is still appropriate. Do you agree? What problems have been encountered as a result of this approach? In what circumstances has it been shown to be helpful or appropriate? What other approaches or combinations of approaches might be more appropriate?

Balancing competing or countervailing interests

2.23 Privacy cannot be an absolute value. Interests in privacy "must be weighed, with complementary and associated interests, against competing public and private interests."[87]

2.24 The UK Committee on Data Protection inquired into privacy in 1978. It neatly states the need to balance competing interests in the area of information privacy as follows:[88]

> though the idea of privacy [was] the starting point for our inquiry its end point is not the construction of a general law of privacy for a legal system which has not yet developed one, but rather the elaboration of a system of data protection which has

86 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 183.

87 Australian Law Reform Commission *Privacy* (ALRC R22, Sydney, 1983) para 44.

88 Report of the Committee on Data Protection (1978) Cmnd 7341, para 18.32, quoted in Tim McBride *Data Privacy: An Options Paper* (Government Printer, Wellington, 1987) para 1.08.

> the protection of privacy as its main objective. Such a system must primarily seek to regulate the flow of information, in order to ensure that those who need information for lawful and reputable purposes can get it freely, while those who do not cannot get it unless the data subject is willing to give it to them…

2.25 In chapter 8 of *Privacy: Concepts and Issues*, we noted that the act of balancing expectations of privacy against other competing interests is particularly demanding, because in some contexts there is a strong public interest in the maintenance of other values that can limit or override privacy.

2.26 The need to balance privacy with other interests is thus put in the ALRC report on privacy:[89]

> As a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience. It is often the case, however, that privacy rights will clash with a range of other individual rights and collective interests, such as freedom of expression and national security. Although the ALRC often heard emphatic arguments couched in the language of rights, international instruments on human rights, and the growing international and domestic jurisprudence in this field, all recognise that privacy protection is not an absolute. Where circumstances require, the vindication of individual rights must be balanced carefully against other competing rights…

2.27 Privacy will not always be in competition with other interests. We noted in *Privacy: Concepts and Issues* that privacy and freedom of information, for example, may sometimes be complementary, such as when freedom from eavesdropping facilitates the exchange of information within a group of trusted associates, or when information can only be gathered in return for an undertaking of anonymity.[90] The congruence of privacy and other interests is also seen in the economic sphere, epitomised in the slogan "privacy is good business". The ALRC translates this by saying "consumer trust is a sine qua non of engagement with such services as e-commerce and internet banking."[91] In some situations, the interests to be balanced will be the individual's own interests. An example is when people's interests in deciding for themselves who accesses their medical records needs to be balanced against their interests in receiving urgent medical treatment when they are incapable of being consulted.

2.28 As we pointed out in *Privacy: Concepts and Issues*, the balancing of privacy interests can be done by the lawmaker itself in the course of formulating rules. Alternatively the lawmaker can transfer responsibility for the balancing exercise to those who apply and enforce the law.[92] Both approaches are evident in the Privacy Act. The first approach (external balancing) is evident in the combination of the information privacy principles and the exceptions to them which is such a central feature of the Act. So when, for example, the Act provides that personal information will not be disclosed unless one of a number of exceptions exists

89 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 104.

90 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 8.7.

91 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 1.74.

92 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 8.19–8.27.

(among them the need to avoid prejudice to the maintenance of the law, or the need to prevent a threat to health) the legislation is itself determining where the balance lies. The exemption for the news media likewise recognises the importance of freedom of information.

2.29 The second approach (internal balancing) can be seen in the provisions of section 14 of the Privacy Act. In carrying out his or her functions, the Privacy Commissioner must, among other things, have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of the free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way, and must also take into account international obligations and any developing international guidelines. This direction is to the Privacy Commissioner, rather than to agencies who are subject to the Act.

2.30 Section 14 is closely based on section 29 of the Australian Privacy Act 1988. In its review of the Australian Act, the ALRC concluded that the Australian Privacy Commissioner, when exercising his or her functions, should continue to have regard to the balance between protecting individual privacy, the desirability of a free flow of information, and minimising compliance costs for government and business.[93] However, the ALRC recommended that these considerations should be incorporated into an objects clause in a new Privacy Act, and that the Commissioner should be required to have regard to the recommended objects of the Act in performing his or her functions and exercising his or her powers.

2.31 Explaining its reasoning, the ALRC stated:[94]

> Aligning the matters to which the Privacy Commissioner must have regard with the objects of the *Privacy Act* ensures that everyone interpreting, applying and attempting to understand the Act—whether they are agencies, organisations, consumers, lawyers, academics or the OPC itself—has regard to the same set of objects. By moving the factors set out in s 29 to the objects clause, the Act effectively indicates that, not only are the enumerated factors critical in influencing the Privacy Commissioner's administration of the Act, they are also critical in directing the general public's understanding and interpretation of the Act.

The Australian Government, in its response to the ALRC report, accepted this recommendation in principle.[95]

2.32 We deal with the issue of incorporating a purpose or objects clause in the New Zealand Privacy Act below.

93 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 46.41–46.46.

94 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 46.46.

95 Australian Government *First Stage Response to the Australian Law Reform Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, 2009) 83.

Q2 Do you think the Privacy Act strikes the right balance between privacy and other competing interests?

Compliance costs

2.33 The Privacy Act, in section 14(a), expressly acknowledges that recognition of the right of government and business to achieve their objectives in an efficient way is one of the social interests that compete with privacy. Despite the slogan that "privacy is good business", in that it promotes good business practice and enhances a business's reputation, it must be acknowledged that the Privacy Act does impose some compliance burden and costs.[96] Good regulatory practice mandates that the design of any regulatory scheme should seek to maximise the benefits or objectives of the scheme while minimising the costs to business and the economy generally.[97]

2.34 We have already referred to the features of the design of the Act that serve to minimise compliance costs. These include the open-textured and outcomes-oriented nature of the Act, through the adoption of a principles-based approach rather than a rules-based approach. Such an approach allows agencies some flexibility in the ways in which they comply with the Act. This approach is reinforced through the adoption of a flexible enforcement regime that promotes settlement and conciliation rather than the imposition of penalties. Codes of practice provide a mechanism for both adapting the Act to specific circumstances, and providing greater certainty through more specific rules.

2.35 Unlike data protection legislation in Europe, the Act does not impose any registration obligations on agencies. Nor does it impose any specific auditing or reporting obligations.[98] In *Necessary and Desirable,* the then Privacy Commissioner commented that the work undertaken by his office in relation to education and publicity, particularly in offering compliance advice, also contributes to minimisation of compliance costs among agencies.[99]

2.36 Compliance costs for small businesses were a particular issue when the Australian Federal Privacy Act was extended to private sector organisations in 2000. While both the New Zealand and Australian Privacy Acts apply to public sector and private sector agencies, the Australian Act exempts small businesses from its coverage (although some small businesses, such as those that trade in personal information, are included). A small business is defined as one that has an annual

96 See further Ministerial Panel on Business Compliance Costs *Finding the Balance: Maximising Compliance at Minimum Cost* (Ministry of Economic Development, Wellington, 2001). The Government's response is contained in *Striking the Balance: Government Response to the Ministerial Panel on Business Compliance Costs* (Ministry of Economic Development, Wellington, 2001).

97 See, eg, *Guidelines on Regulatory Flexibility: Reducing Costs through Compliance Choices and Varied Requirements* (Regulatory Impact Analysis Unit, Ministry of Economic Development, Wellington, 2008).

98 We discuss auditing further in chapter 6.

99 *Necessary and Desirable* 7.

turnover of A$3 million or less. The breadth of the exemption becomes apparent when it is appreciated that up to 94 per cent of Australian businesses may fall under the exemption.[100]

2.37 The ALRC has recommended that the small business exemption in the Australian Act be removed on the basis that it is neither necessary nor justifiable.[101] The ALRC considers that the risks to privacy posed by small businesses are no lower just because the businesses are small. The risks are determined by the amount and nature of personal information that the business holds, the nature of the business, and the way in which the business handles personal information. Further, the small business exemption is a major obstacle to Australia's privacy laws being recognised as "adequate" by the European Union. The Australian Government has not yet responded to this ALRC recommendation.

2.38 The Privacy Commissioner made a number of recommendations in *Necessary and Desirable* for improving ease of use of the Act, which he considered also had the objective of reducing compliance costs.[102] A large number of these are stylistic or drafting issues that we do not deal with here.

2.39 A Ministerial Panel on Business Compliance Costs, in a report produced in 2001, found that:[103]

> Business was concerned that, although its general principles were commendable, the [Privacy] Act did not assist them to apply those principles in everyday work practice. Businesses lost time trying to find out what they are required to do and how to go about it. They were frustrated that simple issues can no longer be resolved by common sense but became complex and time consuming. Calling in expert advice carries a cost. Employers were uncertain what questions they can legitimately ask prospective employees, and whether employees could "hide behind the Act" in their own disclosures. SMEs [small and medium-sized enterprises] were uncertain about the necessity for and the duties of Privacy Officers. Businesses were confused as to which legislation prevails where there is a conflict with the Privacy Act: not many are aware that where that Act is in conflict with another Act such as the Official Information Act, the other Act prevails.

2.40 The Ministerial Panel recommended that the Privacy Commissioner's 0800 helpdesk should be fully staffed at all times, and that the Office of the Privacy Commissioner (OPC) needed to be more proactive generally in providing practical advice. It also recommended that the OPC should prepare step-by-step guidelines and make them readily available. In the Government's response to the Ministerial Panel's report, published in December 2001,[104] the Government agreed with all three recommendations, and reported that the first and second recommendations had already been implemented.

---

100 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1315.

101 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 39.139.

102 *Necessary and Desirable* 7–9.

103 Ministerial Panel on Business Compliance Costs *Finding the Balance: Maximising Compliance at Minimum Cost* (Ministry of Economic Development, Wellington, 2001) 11.

104 *Striking the Balance: Government response to the Ministerial Panel on Business Compliance Costs* (Ministry of Economic Development, Wellington, 2001).

2.41 In a final report-back on the implementation of the Panel's recommendations, published by the Ministry of Economic Development in July 2005,[105] the OPC reported on the initiatives it had taken to respond to the recommendations. These included making available a step-by-step guide to the Act on the OPC website, and the preparation of a *Privacy Impact Assessment Handbook* in both print and electronic formats. That publication was widely distributed through the private and public sectors, and public workshops were undertaken in the main centres on the subject of Privacy Impact Assessments. The OPC had undertaken a number of training workshops within organisations representing a wide range of business sectors, and the OPC's website also provided information about the Act, with that information being updated on an ongoing basis.

2.42 The 2009 Annual Report of the Privacy Commissioner indicates that the OPC's education and publicity activities remain an important focus of the work of the office. The report states:[106]

> Part of the Commissioner's role involves promoting an understanding and acceptance of the information privacy principles. Enquiries officers answer questions from members of the public and maintain an 0800 number so that people may call without charge from anywhere in New Zealand.
>
> The Privacy Commissioner's Office maintains a website (www.privacy.org.nz) that contains many resources, including case notes, fact sheets, newsletters, speeches and reports. Increasingly, enquirers go to the website for information.
>
> Staff give regular workshops and seminars, tailored to the audience, on the Privacy Act, Health Information Privacy Code, security breach guidelines and information matching.
>
> Part of the Commissioner's role is to make public statements on matters affecting privacy, and the Office maintains open communication with the news media. When speaking publicly, the Commissioner may act as a privacy advocate but also has regard to wider and competing considerations.

2.43 Business New Zealand, in conjunction with KPMG, have conducted an annual survey on business compliance costs since 2003.[107] As part of the survey, participants are asked to identify their top compliance cost priorities (categorised into tax, employment, environment, and other). Compliance costs imposed by the Privacy Act do not figure as an identifiable issue in any of these surveys, although it is possible that these costs are included in the more general category of "other" compliance costs.

105 Ministerial Panel on Business Compliance Costs *Final Report-back* (Ministry of Economic Development, Wellington, 2005).

106 Privacy Commissioner *Annual Report of the Privacy Commissioner for the Year ended 30 June 2009* (Office of the Privacy Commissioner ,Wellington, 2009) 17.

107 These surveys are available at www.businessnz.org.nz. The latest survey was published in October 2008.

2.44 A survey was also undertaken in 2004 by Emma Harding as part of an LLB(Hons) research paper on compliance costs under the Privacy Act.[108] The ongoing business costs most widely cited by respondents to that survey were: ensuring staff awareness of the Act's provisions and guidelines; resources devoted to dealing with requests for access to information under the Act; and the cost of obtaining legal advice when required. Nevertheless, Harding found that, despite anecdotal evidence of compliance costs imposed by the Privacy Act, the Act does not impose major compliance costs on New Zealand organisations. Indeed, consistent with the Privacy Commissioner's findings in *Necessary and Desirable*, responses to Harding's survey did not indicate major concerns about compliance costs imposed by the Act. To the extent that the Act does impose compliance costs, Harding concluded that education is the key to reducing those costs.

2.45 As stated above, our preliminary view is that the overall design of the Privacy Act is appropriate. There appears to be no evidence to indicate that any compliance costs arising out of the Act are excessive. Nevertheless, we are keen to hear of ways in which compliance with the Act can be made easier and less costly without compromising the objectives of the legislation.

Q3 Are there ways in which compliance with the Act can be made easier and less costly without compromising its objectives?

NAME, PURPOSE, AND STRUCTURE OF THE ACT

2.46 In this section, we raise issues relating to the name of the Act, the inclusion of a purpose (or objects) clause, and the overall structure of the Act.

What's in a name?

2.47 The Act is simply called the Privacy Act. The Bill that became the Act, when first introduced, was called the Privacy of Information Bill. The select committee recommended that this be changed to Privacy Bill. The select committee considered that, although the Bill related principally to information privacy, the Privacy Commissioner did have a wider role in relation to matters of privacy, and information may not remain the sole focus of the legislation.[109]

2.48 On the assumption that the current scope of the Act remains essentially the same, should it have a name that more closely aligns with its principal focus – information privacy? Would "Information Privacy Act" or "Data Protection Act" be a more appropriate title?

2.49 We note that the Australian Law Reform Commission has recommended that the name of the Privacy Act 1988 (Cth) be changed to the Privacy and Personal Information Act.[110]

108 Emma Harding "Compliance Costs and the Privacy Act 1993: Perception or Reality for Organisations in New Zealand" (2005) 36 VUWLR 529.

109 See para 1.85.

110 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 5.73–5.89, rec 5–3.

2.50 We tend to the view that, because the Act has had its current name for so long, it should not be changed unless there is a compelling reason to do so. The current name is not misleading. Moreover, in our report on stage 3 of this Review we have recommended that the Privacy Commissioner should have a watching brief on surveillance, which would widen the present focus of her activities.[111]

2.51 A related issue is the suitability of the title "Privacy Commissioner". If the name of the Act is considered inappropriate because it suggests that the Act has a wider coverage than it in fact has, is the generality of the title of the Privacy Commissioner similarly inappropriate? If the name of the Act were changed to "Data Protection Act", should the Commissioner be renamed the "Data Protection Commissioner" or something similar?

2.52 We invite comments on these issues.

A new purpose provision?

2.53 The current Long Title of the Act is as follows:

> An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, and, in particular,—
>
> (a) To establish certain principles with respect to—
>
> (i) The collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
>
> (ii) Access by each individual to information relating to that individual and held by public and private sector agencies; and
>
> (b) To provide for the appointment of a Privacy Commissioner to investigate complaints about interferences with individual privacy; and
>
> (c) To provide for matters incidental thereto.

2.54 Our current thinking is that, even if major changes to the current Act are not warranted, the Act should be replaced with a new Act drafted in a more modern and up-to-date style. Since 2000, new Acts no longer contain a Long Title. Their modern equivalent is a purpose or objects clause. According to the Parliamentary Counsel Office's Drafting Manual, the aim of a purpose clause is to assist with the understanding of the Act.

2.55 As noted above, the ALRC has recommended the inclusion of an objects clause in the Australian Federal Privacy Act, setting out the purpose and aims of the legislation.

111 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, Wellington, 2010) 58 (R18).

2.56 If a new purpose clause were to simply incorporate the content of the current Long Title, it might look like this:

> **Purpose of this Act**
>
> The purpose of this Act is to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, and, in particular,—
>
> (a) To establish certain principles with respect to—
>
> (i) The collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
>
> (ii) Access by each individual to information relating to that individual and held by public and private sector agencies; and
>
> (b) To provide for the appointment of a Privacy Commissioner to investigate complaints about interferences with individual privacy; and
>
> (c) To provide for other incidental matters.

2.57 However, we have noted above that the ALRC recommended that the substance of the Australian equivalent of our section 14 be included in the purpose provision. We in New Zealand might also include a provision which acknowledges that privacy is not an absolute value, and that one of the purposes of the Act is to strike the appropriate balance between privacy and other values. Such a clause might read:

> To recognise that the right to privacy is not absolute, and to achieve an appropriate balance between that right and other important human rights and social and economic interests that compete with it.

This might operate as a useful disincentive to treating privacy as the be-all and end-all, indicating that it is indeed subject to exceptions.

2.58 It might be appropriate to include other matters in an objects clause. For example, the ALRC recommends that an objects clause in the Australian Act should recognise the relationship between the protection of privacy and electronic commerce. It considers that this would reflect a number of international instruments that have been developed in this area, such as the OECD Guidelines, the EU Directive, and the APEC Privacy Framework. So a further objective of the Australian Act would be "to facilitate the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy."[112]

2.59 We invite comment on what a new purpose clause in a rewritten Privacy Act should contain.

112 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) Recommendation 5–4.

Structure

2.60 In *Necessary and Desirable*, the then Privacy Commissioner made a number of recommendations, the objective of which was to make the Act easier to use.[113] Some of these recommendations relate to structural matters. These include:

- making headings to sections, parts, principles, and rules more helpful, accurate, and precise;
- recasting certain definitions; and
- clarifying the relationship between the Act and other enactments by relocating certain provisions or incorporating certain content into the privacy principles themselves.

2.61 The significance and wide application of the Act make it particularly important that the Act is as navigable, readable, and understandable as possible for those who want to take advantage of it, those who have to comply with it, and those who have to enforce it. Rewriting the Act in a more modern and up-to-date drafting style will assist. We also welcome comments on how the Act might be better structured so that it is easier to navigate and to read.

Q4 Should the name of the Privacy Act be changed? If so, what should its new name be? Should the Privacy Commissioner be called something else, such as the Data Protection Commissioner?

Q5 Should the Privacy Act contain a purpose clause? If so, what should it say?

Q6 How might the Privacy Act be better structured so that it is easier to navigate and to read?

PERCEPTIONS AND MISUNDERSTANDINGS

2.62 Since its enactment, the Privacy Act has attracted some criticism from the news media and others, principally over what are perceived to be the Act's undue restrictions on freedom of information. Tim McBride, in an article published in 1998, stated that, in the Privacy Act's short life, "there has been no shortage of incidents where the Act has been portrayed – sometimes quite unfairly – as the 'enemy' of the 'public's right to know'".[114] A 1997 article on the Privacy Act in *Consumer* magazine, sparked by the Privacy Commissioner's investigation into a case involving a nurse releasing an individual's medical records to a politician, stated of the news media's reporting of that investigation: "The Privacy Act, as is often the case, was cast as a law that prevents common sense from prevailing and justice from being done."[115]

113 *Necessary and Desirable* 7–9.

114 Tim McBride "News Media and the Privacy Act" [1998] PLPR 79.

115 "Mind Your Own Business" (June 1997) *Consumer* New Zealand 35.

2.63 More recently, the Privacy Act has been blamed for preventing:

- parents from finding out about the activities of their teenage children;[116]
- Police from gathering information that could assist with detecting the manufacture of the drug "P";[117]
- a boarding house manager from knowing about a tenant's previous conviction for a rape that occurred in another boarding house;[118] and
- sharing of information that could help to detect or prevent child abuse.[119]

2.64 By contrast, another story, which portrayed the Privacy Act as inadequately protecting the privacy of personal information, discussed the release of the personal details and trading history of up to 10,000 Trade Me users to defendants in a prominent criminal case. The records had been obtained from Trade Me by the Police under a search warrant, and made available to defence counsel. The records even ended up in the prison cell of one of the defendants. Although the article correctly points out that the Privacy Act is subject to criminal discovery and other laws, the author of the article still implies that the Act is at fault in this situation by stating: "Those who expected the Privacy Act to protect their information will be disappointed."[120]

2.65 The ALRC, in its review of the Australian Federal Privacy Act, refers to the "BOTPA" (because of the Privacy Act) excuse.[121] This, it says, is where privacy is cited as an excuse for inaction or non-cooperation, rather than as a genuine reason for refusing to disclose information. It would not be difficult to find New Zealand examples of people wrongly sheltering behind the Act.

2.66 How a piece of legislation is perceived by those who are affected by it, and by the public at large, is an important consideration in reviewing how the legislation is working in practice. That said, there will inevitably be cases in which legislation is misinterpreted or misapplied. In a number of cases which have attracted criticism it has been the failure of an agency to understand or apply the Act correctly that has been the cause of the problem, rather than the Act itself. These cases will colour the general public's perception of the scope and application of the legislation, regardless of the correct legal position. As with the issue of compliance costs examined above, the role of the Privacy Commissioner in educating the public about the Act is therefore of critical importance.

2.67 As part of our review of the Act, we are concerned to understand where the Act might need changing, not only to improve its actual legal effectiveness but also so that the public perception and understanding of the Act might more correctly

116 Jane Phare "Teen Machine" (6 January 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 3 February 2010).

117 Beck Vass "Privacy Laws Snarl Plans for Pharmacy Drug-watch System" (23 October 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 3 February 2010).

118 Jonathan Marshall "Paroled Backpacker Rapist Moved from Hostel" (28 January 2007) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 3 February 2010).

119 Bob Harvey, Mayor of Waitakere (Speech to the Every Child Counts Conference, Wellington, 10–11 September 2008).

120 David Fisher "Raid Me" (9 August 2008) *The Listener* www.listener.co.nz (accessed 3 February 2010).

121 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 109–110.

match its objectives, scope, and application. We therefore particularly welcome feedback on how the Act is perceived to be operating in practice. Real-life examples are especially useful.

Q7 How is the Act perceived to be operating in practice? Are any perceived deficiencies the result of the Act itself, or rather of the way it is understood and applied? Could any changes to the Act be made so that the public perception and understanding of it more correctly match its objectives?

PRIVACY COMMISSIONER GUIDANCE

2.68 We noted above that the Privacy Commissioner has a statutory power to make codes. These are a form of delegated legislation, and have the force of law. Breach of them has the effect of a breach of a privacy principle.

2.69 As we have also explained earlier in this chapter, the Privacy Commissioner often also issues guidelines and other forms of advice and guidance. No statutory authority is needed for this: an official can always give advice. But if statutory authority were to be sought, it can be found in sections 13(1)(a) and 13(1)(l) of the Privacy Act. They confer functions "to promote …understanding and acceptance of the information privacy principles" and "to provide advice …to a Minister or an agency on any matter relevant to the operation of this Act".

2.70 The Privacy Commissioner has in fact issued much guidance. There are booklets: *Privacy in Schools* (written for the Commission by Kathryn Dalziel),[122] and *Privacy at Work.*[123] There is website guidance on composing privacy notices, a brochure for businesses entitled *Privacy is Good Business*, and a brochure for health consumers. Much more formal in tone and appearance are the sets of guidelines, *Privacy and CCTV,*[124] and *Key Steps for Agencies in Responding to Privacy Breaches.*[125] These publications are made up of sets of numbered guidelines, and take on more of the appearance of legislative instruments. Yet they are not. Failure to comply with their provisions does not itself amount to an interference with privacy. They are simply a statement of good practice, and advice on how to keep within the law.

2.71 Many statutory regulatory agencies have power both to make rules and to issue non-binding guidelines. At times, the line between the two can be shadowy: indeed, guidelines and similar non-binding documents are occasionally called by the rather unfortunate name of "soft law". There is a danger that since they emanate from an official source, they may be regarded as binding law by those who read them.

122 Kathryn Dalziel *Privacy in Schools: A guide to the Privacy Act for Principals, Teachers, and Boards of Trustees* (Office of the Privacy Commissioner, Wellington, 2009).

123 Office of the Privacy Commissioner *Privacy at Work: A guide to the Privacy Act for employers and employees* (Wellington, 2008).

124 Office of the Privacy Commissioner *Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations* (Wellington, 2009).

125 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, 2008).

2.72 However, provided their nature and effect is understood (and the Privacy Commissioner's documents do make it clear that their purpose is to *encourage* and *assist*) such guidance documents are most valuable. They help to flesh out the general principles in the Act. Indeed, throughout this issues paper, we ask whether further guidance on various matters could usefully be issued by the Privacy Commissioner. Such a light-handed approach is often more satisfactory than laying down rules in the form of a code.

2.73 Yet two things must be borne in mind. First, the preparation of guidelines involves much time and resource. The Privacy Commissioner's resources are limited. Secondly, the Privacy Commissioner is not the only person who is entitled to provide guidance. In certain matters (record-keeping for example) it may be appropriate for some other agency (Archives New Zealand, for instance) to do it, in consultation with the Privacy Commissioner. At times industry bodies can also appropriately provide useful advice, an example being the Code of Practice for Direct Marketing prepared by the Marketing Association of New Zealand in conjunction with the Advertising Standards Authority, and in consultation with a number of government agencies.

Q8 Do you find the guidance issued by the Privacy Commissioner useful? On what topics would you like more such guidance?

Chapter 3
Key definitions

3.1 Section 2 of the Privacy Act defines various terms used in the Act. Some of these terms are discussed elsewhere in this issues paper. Here we discuss three key terms that are central to the scope and coverage of the Act as a whole: "personal information", "individual" and "collect". At the end of the chapter we ask whether there are any other terms whose meaning for the purposes of the Act should be amended or clarified.

"PERSONAL INFORMATION"

3.2 The definition of "personal information" in the Privacy Act is very broad, and is not limited to information that is particularly sensitive, intimate or private. Nor does the Act have a separate category of "sensitive information", as some overseas privacy legislation does. The Act defines personal information as "information about an identifiable individual". It goes on to state that the definition includes information about a death maintained pursuant to the Births, Deaths, Marriages and Relationships Registration Act 1995 (as discussed later in the chapter). "Individual" is separately defined, and is discussed in a later section of this chapter.

3.3 The definition of personal information is central to establishing the scope of the Privacy Act, yet Katrine Evans has commented that "deciding what is, and what is not 'personal information' can be one of the hardest legal calculations in everyday privacy practice."[126] It is important to emphasise at the outset, however, that in most cases it will be quite clear whether information is "personal information" or not. We are not aware of the definition of personal information causing major problems in the day-to-day application of the Act by agencies. Ambiguity and uncertainty arise only at the margins; but those margins can be very important in particular cases, and for establishing the boundaries of the Act's coverage. In this section we ask: to what extent is the definition of "personal information" inherently complex and ambiguous, and to what extent could it be clarified in the statute or by some other means? Some areas of ambiguity are discussed below.

126 Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner "Personal Information in New Zealand: Between a Rock and a Hard Place?" (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 1.

"Information"

3.4 "Information" is not defined in either the Privacy Act or the Official Information Act 1982 (OIA). The leading New Zealand authority on the meaning of information is the definition given by McMullin J in *Commissioner of Police v Ombudsman*: "that which informs, instructs, tells or makes aware".[127] To constitute information, something must be capable of being understood; a person must be able to derive meaning from it. Some writers have drawn a distinction between "data" and "information". Raymond Wacks writes that: "'Data' become 'information' only when they are communicated, received, and understood. 'Data' are therefore potential 'information'."[128] Paul Roth draws a similar distinction, writing that:[129]

> "information" may be contrasted to mere "data" in that information is always "about" something or someone, while data are the raw material or building blocks that comprise "information". Information can therefore be conceived of as "data" that have been "processed" in some way, and the essence of "information" is that it conveys meaning or, as one author has termed it, "aboutness". Information can be viewed as data placed in context and made meaningful or useful in some way.

There is something to this distinction, although we would caution against attaching any significance to the fact that the New Zealand Privacy Act is concerned with "personal information" while some overseas statutes (particularly in Europe) use the term "personal data": we think both terms are generally used to mean the same thing in information privacy laws around the world.[130]

3.5 It seems to be undisputed that "personal information" covers information collected or held in a wide range of forms, including audio and visual recordings. We believe that it does not cover bodily samples (as distinct from information obtained from those samples), as discussed further below.

3.6 Personal information for the purposes of the Privacy Act is not limited to information that has been recorded in some form, and most of the authority in cases relating to the OIA, the Local Government Official Information and Meetings Act 1987 and the Privacy Act is that unrecorded matter held in a person's mind can be "information".[131] The inclusion of information that exists only in a person's mind appears to set the New Zealand Privacy Act apart from most overseas privacy legislation. For example, the definition of "data" in the Data Protection Act 1998 (UK) is limited to information which is recorded or is being automatically processed by machine (which implies that it must exist in some sort of record recognisable by the machine).[132] The definition of "personal information" in the Privacy Act 1988 (Cth) expressly states that it includes

127 *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385, 402 (CA) McMullin J.

128 Raymond Wacks *Personal Information: Privacy and the Law* (Clarendon Press, Oxford, 1989) 25.

129 Paul Roth "What is Personal Information?" (2002) 20 NZULR 40, 51.

130 Indeed, the Data Protection Act 1998 (UK), s 1(1), defines "data" as meaning certain types of "information".

131 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12, 152,203–152,207.

132 Data Protection Act 1998 (UK), s 1(1).

information "whether recorded in a material form or not",[133] but this provision is limited by other provisions in the Act which restrict the Act's application to information that is being collected for inclusion in a "record", or is held in a "record".[134] In New South Wales, the Privacy and Personal Information Act 1998 similarly states that "personal information" includes information "whether or not recorded in a material form",[135] and the Act's application is not limited in the same way as is the Federal Act's. This opened the door for both the Administrative Decisions Tribunal and that Tribunal's Appeal Panel to find that personal information could include information held in a person's mind. However, this finding was overturned on appeal to the Court of Appeal, with Spigelman CJ holding that:[136]

> Of particular significance is the body of consecutive sections between s12 and s19 of the Privacy [and Personal Information] Act which adopt as their criterion of operation a reference to where a public sector agency "holds personal information"…. It is almost impossible to conceive how almost all of those … sections could operate in practice if they were intended to apply to information in the minds of employees acquired by direct visual or aural experience and never recorded in any manner.

3.7 The New South Wales Court of Appeal decision raises some interesting questions about the implications of treating information held in a person's mind as personal information for the purposes of the Privacy Act. On the one hand, knowledge and opinions held in a person's mind are clearly information, and treating them as such for the purposes of the Act enhances people's rights under the Act. For example:

- When people seek access to information about themselves held by an agency (principle 6), that information may include material that has not been recorded but does nonetheless influence an agency's dealings with an individual. Indeed, excluding undocumented information could create an incentive for agencies not to keep a record of meetings or other interactions that concern a particular individual, or to destroy such records.
- Principle 11 deals with disclosure of personal information. Disclosure of information that is not contained in a recorded form can be just as harmful as disclosure of information in writing, in a photograph, or in another type of document.
- The requirement to check the accuracy of personal information before use (principle 8) is just as important if that information is held in a person's mind as it would be if the information were recorded in some way.

3.8 On the other hand, there are some conceptual and, perhaps, practical difficulties with including information held in a person's mind in the Act's coverage. For example:

- How can the purpose for which such information is held be established?
- How can the security of such information be protected (principle 5)?
- If such information is incorrect, how can it be corrected (principle 7)?
- How can an agency ensure that the information is not kept for longer than is necessary (principle 9)?

---

133 Privacy Act 1988 (Cth), s 6(1).

134 Privacy Act 1988 (Cth), ss 14, 16B.

135 Privacy and Personal Information Act 1998 (NSW), s 4(1).

136 *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192, para 28.

3.9 Some of these difficulties may be more theoretical than real, and a number of features of the Act help to deal with any potential problems. In particular:

- A number of the privacy principles require agencies to take only such action as is reasonable in the circumstances.
- Information held in the mind of an individual will not necessarily be held by the agency for which that individual works or of which that individual is a member.[137]
- With regard to access requests under principle 6, a request may be refused if the information "is not readily retrievable" or "cannot be found".[138] This may sometimes be the case where information held in a person's mind is concerned.

3.10 Nonetheless, evidential problems may arise, as Paul Roth notes:[139]

> Once it is accepted that the Privacy Act covers information that is not in documentary form, evidential issues will inevitably arise in relation to whether personal information is actually held; whether it is "readily retrievable"; whether it has been fully disclosed in response to a Principle 6 request; and whether it has been disclosed in breach of Principle 11.

In *A and A v G*, the Complaints Review Tribunal considered a complaint involving information disclosed in the course of a conversation. The Tribunal commented that the definition of personal information in the Act:[140]

> carries within it the specific implication that the information the subject of any issue raised by the Act is itself known, accepted or understood in very precise terms. This will generally not pose a problem where the information at issue is recorded in some way. There is, however a difficulty when the precise nature of the personal information is not known, accepted, or understood in precise terms. That is a difficulty which is likely to arise in respect of personal information which is not recorded but which is held in the memory of an individual.

3.11 The Law Commission would be interested to hear, as part of submissions on the definition of "personal information", whether the inclusion of information held in a person's mind in the definition of personal information causes practical problems for agencies, and whether such information should continue to be covered by the definition.

3.12 Other questions are whether information includes opinions and false information. With regard to false information, it seems clear that this is covered by the Privacy Act, and that whatever limitations there may be with regard to the privacy tort's coverage of false information do not apply in the Privacy Act context. If false information did not fall within the coverage of "personal information", principle 7 (which concerns correction of inaccurate information) would be nonsensical. There also seems to be no reason why opinions cannot be information, although they are not expressly included in the definition of personal information.

---

137 Privacy Act 1993, ss 3–4.

138 Privacy Act 1993, s 29(2)(a) and (b); see also the terms of principle 6 itself.

139 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12, 152,401.

140 *A and A v G* (13 July 1999) Complaints Review Tribunal 18/99, 6.

3.13 The fact that the Privacy Act contains no definition of "information" does not seem to have created significant problems. However, it could be worthwhile to put certain matters beyond doubt by amending the definition of "personal information" to include elements found in the Privacy Act 1988 (Cth):[141]

- "information *or an opinion*";
- "whether true or not"; and
- "whether recorded in a material form or not" (although we believe that a better form of words for the New Zealand Act would be "whether recorded in a document or not", since "document" is fully defined in the Act).

It is also worth noting that the definition of "personal information" in the Privacy of Personal Information Bill recently introduced in South Africa expressly includes both "the personal opinions, views or preferences of the person" and "the views or opinions of another individual about the person".[142]

"About"

3.14 Whether information is "about" an identifiable individual or not is probably the question that gives rise to the most uncertainty in the application of the definition of "personal information". It also appears to be the most difficult issue to resolve or clarify through amending the statute. Questions concerning whether information is "about" an individual seem to arise most commonly in access cases, where decisions have to be made about whether particular information is personal information about the requestor that should therefore be released to him or her. However, they can also arise in cases concerning breaches of other privacy principles.

3.15 In obiter comments in *Harder v Proceedings Commissioner*, the majority in the Court of Appeal appeared inclined to read down the meaning of "personal information" by limiting it to information that is "about" an individual in a fairly narrow sense.[143] There is no authoritative decision on this point in New Zealand, but an indication of how the courts could narrow the scope of personal information by reference to the requirement that the information be "about" an individual can be found in the English case of *Durant v Financial Services Authority*. In that case, the Court of Appeal held that whether or not mention of a data subject in a document amounts to his 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". The Court stated that two notions could be of assistance in this respect:

---

141 Privacy Act 1988 (Cth), s 6. The ALRC has recommended keeping these aspects of the definition of "personal information" unchanged: Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 306, 309 (rec 6–1).

142 Protection of Personal Information Bill (South Africa), cl 1, definition of "personal information", subclauses (e) and (g).

143 *Harder v Proceedings Commissioner* [2000] 3 NZLR 80, paras 23–24 (CA) Tipping J; however, see the contrary view of Gault J at para 49. The Court's obiter comments on the meaning of "personal information" have been questioned by some commentators: see Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner "Personal Information in New Zealand: Between a Rock and a Hard Place?" (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 5; Paul Roth "What is Personal Information?" (2002) 20 NZULR 40, 43–45.

- whether the information "is biographical in a significant sense", that is, whether it has personal connotations and could compromise his or her privacy, or merely records his or her involvement in some matter or event; and
- whether the information has the individual as its focus, or whether it actually has as its focus some other person with whom the individual may have been involved or some event in which he or she may have figured or had an interest.

"In short," the Court concluded, "it is information that affects his privacy, whether in his personal or family life, business or professional capacity."[144] This narrow interpretation of the meaning of "personal data" has been criticised by a number of commentators.[145]

3.16 In technical guidance on the meaning of personal data,[146] the UK Information Commissioner has attempted to reconcile the finding of the Court in *Durant* with the much broader definition of personal data in an Opinion of the European Union Article 29 Data Protection Working Party.[147] The Article 29 Working Party Opinion distinguishes between three elements which, if any one of them is present, indicate that data "relate" to an individual (which is the terminology of the EU Data Protection Directive). Only one of these elements, the "content" element, concerns whether the information is "about" an individual in the sense that it involves his or her personal details, characteristics, activities and so on. The other two elements concern whether the information will be used to evaluate, treat in a certain way, or influence the status or behaviour of an individual; or whether the use of the information is likely to have an impact on an individual's rights or interests.[148]

3.17 With the exception of the obiter comments in *Harder*, New Zealand courts and the Human Rights Review Tribunal have not so far shown any inclination to take the narrow approach of the English Court of Appeal in *Durant*. However, a distinction between information "about" an individual and information that in some way relates to an individual was drawn by the Human Rights Review Tribunal in *CBN v McKenzie Associates*. While declining to draw any final conclusions about the scope of "personal information", the Tribunal commented that "The fact that information may become relevant to someone does not necessarily convert it into information 'about' that person." In the particular case in question, information about the plaintiff's wife held on the defendants' file "may have been relevant to the plaintiff in the sense that it might have either

144 *Durant v Financial Services Authority* [2003] EWCA Civ 1746, para 28 Auld LJ.

145 See, for example, David Lindsay "Misunderstanding 'Personal Information': *Durant v Financial Services Authority*" [2004] PLPR 13.

146 *Data Protection Technical Guidance: Determining What is Personal Data* (UK Information Commissioner's Office, 2007).

147 Richard Cumbley and Peter Church "EU – What is Personal Data?" (October 2008) *Technology, Media & Telecommunications News* www.linklaters.com (accessed 30 July 2009). The UK Information Tribunal has commented that it has "difficulty in reconciling the approach in the Guidance with that in Durant": *Harcup v Information Commissioner and Yorkshire Forward* (5 February 2008) Information Tribunal (UK) EA/2007/0058, para 20.

148 Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 10–11.

limited or enhanced his chances of obtaining the custody arrangements that he wanted", but the Tribunal "struggle[d] to see" that that information thereby became information "about" the plaintiff.[149]

3.18 Examples of difficult questions with regard to when information is "about" an individual include:[150]

- Are exam scripts information about the students who wrote them? What about the exam questions – in responding to an access request, can an agency legitimately provide copies of the answers without the questions?
- Assuming that opinions are "information", is A's opinion of B personal information about A, about B, or about both of them?
- In what circumstances can information about other people be information about an individual? If information about another person is relevant to a decision that is made about person A, does that make it information about person A? (For example, information about the successful candidate for a job for which A applied unsuccessfully.)
- In what circumstances can information about an object be information about a person? (For example, an insurance report about a mechanic's repairs to a person's car, in the context of a dispute over the adequacy of the repairs.)
- If an agency has a file about an individual, should everything in that file be considered to be about the individual, or can it properly be separated into information that is about the individual and information that is not?
- To what extent, and in what circumstances, are minutes of meetings information about the participants in the meeting?

3.19 The answer to questions such as these seems to be: it all depends on the context. The Human Rights Review Tribunal acknowledged as much in *CBN v McKenzie Associates*:[151]

> there is no "bright line" test which separates that which is obviously personal information about an identifiable individual from that which is not. Much will depend in any given case on the context in which the information is found.

It seems unlikely that it would be either possible or desirable to amend the definition of "personal information" to provide clarification with regard to what makes something information "about" an individual. Guidance from the Privacy Commissioner, like that produced by the Information Commissioner in the UK, is an option that could be considered, however.

149 *CBN v McKenzie Associates* [2004] NZHRRT 48, para 39.

150 For further discussion of these and other examples see Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner "Personal Information in New Zealand: Between a Rock and a Hard Place?" (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 8–9; Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12; Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 9–12; *Data Protection Technical Guidance: Determining What is Personal Data* (UK Information Commissioner's Office, 2007) 9–17.

151 *CBN v McKenzie Associates* [2004] NZHRRT 48, para 41.

"Identifiable"

3.20 It is significant that the definition of personal information requires only that the individual be "identifiable", not that he or she be "identified" in the information. Even so, there could be a question as to whether the individual must be identifiable from the internal evidence of the information in question alone, or whether the individual could be identifiable from the information in question in combination with other information. According to Paul Roth, the Ombudsmen, the Privacy Commissioner and the courts have taken the latter approach to the question of identifiability. Roth further argues that the approach of not requiring that individuals be identifiable from the information in question alone is consistent with overseas legislation and international standards, and is supported by certain features of the Privacy Act itself.[152]

3.21 If it is accepted that this approach is the right one, at least two areas of uncertainty remain. First, by whom must the individual be identifiable? Must the individual be identifiable to casual observers, or is it enough that he or she could be identified by close friends or family? What if the individual can only be identified by himself or herself? It seems that the individual does not necessarily have to be identifiable to the world at large, and it can be enough that he or she can be identified by those who know him or her. In *Proceedings Commissioner v Commissioner of Police*, the Complaints Review Tribunal did not accept the argument:[153]

> that an identifiable individual's privacy should not be regarded as breached if an identification can only be made as a result of prior knowledge by some members of the public of an individual. We think this would limit identifiability to identification by strangers and we do not accept that this is what the definition of personal information says.... It is enough that they are able to be identified by anyone who can make an identification as the result of the receipt of personal information not previously known.

Where the individual can be identified only by himself or herself, the Privacy Commissioner has formed the opinion that there is no personal information involved.[154] However, Paul Roth argues that this view is mistaken: in such a case the information can still be personal information, and the fact that no one else can identify the individual should instead be taken into account when assessing the question of harm.[155]

3.22 The second area of uncertainty concerns the means and practicality of identification. In other words, is it reasonably practicable, rather than merely theoretically possible, to identify the individual? Some international instruments,

152 Paul Roth "What is Personal Information?" (2002) 20 NZULR 40, 48–50.

153 *Proceedings Commissioner v Commissioner of Police* (16 December 1999) Complaints Review Tribunal 37/99.

154 *Man Complains About Publication of his Photograph in a Booklet* [2006] NZPrivCmr 7 – Case Note 64131; Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner "Personal Information in New Zealand: Between a Rock and a Hard Place?" (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 3.

155 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12, 152,404–152,405.

and legislation and guidance from other jurisdictions, provide greater assistance with regard to this question than does the New Zealand Privacy Act. For example:

- The definition of personal data in the Hong Kong Personal Data (Privacy) Ordinance refers to information from which an individual's identity can "practicably" be directly or indirectly ascertained.[156] Likewise, some Australian statutes refer to information from which a person's identity can "reasonably" be ascertained.[157]
- The Data Protection Act 1998 (UK) refers to data relating to an individual who can be identified from the data alone, or from the data "and other information which is in the possession of, or is likely to come into the possession of, the data controller".[158]
- Recital 26 of the EU Data Protection Directive states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the [data] controller or by any other person to identify the said person".[159]
- Elaborating on the statement in the EU Directive, guidance from the UK Information Commissioner states that "the fact that there is a very slight hypothetical possibility that someone might be able to reconstruct the data in such a way that the data subject is identified is not sufficient to make the individual identifiable for the purposes of the Directive." However, assessing identifiability does not involve simply considering the means reasonably likely to be used by the average person in the street, "but also the means that are likely to be used by a determined person with a particular reason to want to identify individuals".[160]

3.23 Similar statements, either in the Privacy Act or in guidance from the Privacy Commissioner, could assist in New Zealand. Assistance could also be provided by listing some factors to be taken into account in assessing the practicality of ascertaining a person's identity. Microsoft Asia Pacific, in a submission to the Australian Law Reform Commission (ALRC), stated that the reasonableness test:[161]

> necessitates a consideration of the cost, difficulty, practicality and likelihood of the organisation linking information with other personal information accessible to it, and not merely whether the organisation would be able to link the information after incurring substantial expenditure.

156 Personal Data (Privacy) Ordinance (Hong Kong), s 2.

157 Privacy Act 1988 (Cth), s 6; Privacy and Personal Information Act 1998 (NSW), s 4; Information Privacy Act 2000 (Vic), s 3.

158 Data Protection Act 1998 (UK), s 1(1).

159 EC Directive 95/46/EC.

160 *Data Protection Technical Guidance: Determining What is Personal Data* (UK Information Commissioner's Office, 2007) 7.

161 Microsoft Asia Pacific, submission to the ALRC, quoted in Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 301; at 308 the ALRC states that this "is an appropriate formulation of the test".

Similarly, a Council of Europe Recommendation states that: "An individual shall not be regarded as 'identifiable' if the identification requires an unreasonable amount of time, cost and manpower."[162]

3.24 The issue of identifiability is further complicated by the increasing ease with which anonymised or deidentified information can be reidentified. Computers have made it easier to analyse data and find unique "data fingerprints" within it, but perhaps even more importantly the internet has made a vast amount of data readily available, so that data fingerprints can be combined with other information in order to identify the individuals to whom those fingerprints correspond. In a recent article, American legal academic Paul Ohm has argued that, as a result of advances in reidentification, the concept of "personally-identifiable information" (PII) on which laws like the Privacy Act depend has been rendered meaningless. PII is an ever-expanding category, according to Ohm, and should therefore be rejected as a basis for information privacy regulation. Instead, he argues, privacy law should be based on assessing risks of harm in specific contexts and weighing those risks against the benefits of free flows of information in those contexts.[163] Ohm's article is a major challenge to one of the key concepts underlying information privacy law around the world, and the problems he identifies will probably become more acute over time.

A particular issue: Internet Protocol (IP) addresses

3.25 As with other elements of the definition of personal information, context will often be very important in determining whether or not a piece of information is linked to an identifiable individual. One example of the importance of context is the issue of whether an Internet Protocol (IP) address can be information about an identifiable individual, a question about which there has been much debate. Strictly speaking, an IP address identifies a computer or other internet-connected device, not a person (just as, strictly speaking, a street address identifies a house, not the owner or inhabitant of the house). On its own, therefore, an IP address could be considered not to constitute personal information. IP addresses can be static (that is, the address stays the same each time the user connects to the internet) or dynamic (meaning that the address changes each time the user connects to the internet). Regardless of whether the address is static or dynamic, the Internet Service Provider (ISP) will know the identity of the person or organisation holding the subscriber account to which the IP address has been assigned (although that person may not be the user at any given time).[164] It is also arguable that, even if the user's identity as a living individual is not known, his or her online activity is identifiable by means of the IP address for purposes such as targeting of online advertising.[165]

---

162 Council of Europe Recommendation on Communication to Third Parties of Personal Data Held by Public Bodies (9 September 1991) R(91)10, quoted in Paul Roth "What is Personal Information?" (2002) 20 NZULR 40, 50.

163 Paul Ohm *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (University of Colorado Law Legal Studies Research Paper No 09–12, 2009), available at www.ssrn.com.

164 Rosemary Jay and Louise Townsend "IP Addresses and the Data Protection Act" (March 2008) www.out-law.com (accessed 29 July 2009).

165 "Hustinx: Nameless Data Can Still be Personal" (6 November 2008) www.theregister.co.uk (accessed 29 July 2009).

3.26 There have been a range of views on whether an IP address is personal information. Some decisions in overseas jurisdictions have held that IP addresses are not personal information because they do not directly identify individuals.[166] The Article 29 Data Protection Working Party, on the other hand, considers that IP addresses are data relating to identifiable individuals. The Working Party acknowledges that in some cases (such as computers at internet cafes), the individual using the computer will truly not be identifiable from the IP address, but considers that unless an ISP is in a position to know with certainty that particular data corresponds to unidentifiable users it should treat all IP information as personal data, "to be on the safe side".[167] The ALRC takes a middle-ground position, arguing that information that would allow an individual to be contacted (such as a phone number, street address or IP address in isolation) is not personal information, but that "such information may come to be associated with a particular individual as information accretes around the number or address."[168] It seems that whether an IP address is personal information or not is a matter that can only be decided in relation to the particular context in which that address is collected, held, used or disclosed. It is probably not a matter that can be clarified by an amendment to the Privacy Act, although guidance from the Privacy Commissioner could be considered.

Options for clarifying the definition of "personal information"

3.27 There are three options for dealing with the areas of uncertainty in relation to the definition of "personal information" discussed above:

- the definition in the Act could be amended;
- the Privacy Commissioner could provide official guidance on the definition; and
- the resolution of areas of uncertainty could be left to Commissioner case notes and decisions of the Tribunal and the courts.

3.28 There is room for each of these options to be used for different issues. Some matters can probably be clarified by amending the definition. These may be matters on which there is already a consensus in opinions of the Commissioner and decisions of the Tribunal and courts, but this does not mean that it is not worthwhile. For one thing, it would put matters beyond doubt, and help to avoid the generally-understood position being overturned in the courts. There is also value in the Act being as explicit as possible, since it has to be applied by countless

166 See for example Wendy David "Court: IP Addresses are not 'Personally Identifiable' Information" (6 July 2009) www.mediapost.com (accessed 29 July 2009); "IP Address Alone May Not Be 'Personal Data'" (summary of a decision of the Hong Kong Privacy Commissioner for Personal Data and subsequent appeal) in Privacy Commissioner for Personal Data *Annual Report 2007–08* (Hong Kong, 2008) 79–81.

167 Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 16–17. See also the views of EU Data Protection Supervisor Peter Hustinx: "Hustinx: Nameless Data Can Still be Personal" (6 November 2008) www.theregister.co.uk (accessed 29 July 2009). However, some courts in EU states have held that IP addresses are not personal data, as have some European data protection regulators: Richard Cumbley and Peter Church "EU – What is Personal Data?" *Technology, Media & Telecommunications News* (October 2008) www.linklaters.com (accessed 30 July 2009); Paul Ohm *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (University of Colorado Law Legal Studies Research Paper No 09–12, 2009) 59.

168 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 308–309.

individuals who do not have the time to familiarise themselves with Privacy Act jurisprudence. Examples of matters that could be made clear in the definition are that "personal information" includes opinions, false information, and information not recorded in a material form. It might also be possible to provide clarification in the statute with regard to identifiability, particularly on the question of the practicality of identification.

3.29 Guidance from the Privacy Commissioner could be helpful in clarifying the meaning of "personal information" and assisting agencies to work through whether particular information is covered by the Act or not. Where matters cannot easily be clarified in the statute itself, official guidance from the Commissioner could help to fill some gaps and address specific issues such as IP addresses. It could also use examples, as the guidance from the UK Information Commissioner and the Opinion of the EU Working Party do. However, in addition to the resourcing implications for OPC of developing and consulting on guidelines, there are some potential risks that should be considered. One is that the guidance could be too prescriptive, or could be applied in an overly-mechanical way. It will always be important for the meaning of personal information to be considered in relation to the particular context, and to be applied flexibly so as to be consistent with the spirit and intention of the Act. There is a danger that the guidance could assume more importance than the law itself, and could introduce rule-based regulation by the back door. The other risk is that guidance from the Privacy Commissioner could diverge from authoritative rulings of the courts, as appears to have happened in the UK following the *Durant* decision.

3.30 Leaving the meaning of personal information to be clarified through opinions and decisions in particular cases has the advantage of flexibility. There are also some issues (such as the meaning of "about") that can probably only ever be resolved in relation to the facts of specific cases. However, it takes time for a consensus to develop in the jurisprudence, or for a suitable case to lead to an authoritative court decision. Clarifying the meaning of the Act through jurisprudence is also less accessible to users of the Act than stating matters in legislation or official guidance.

3.31 The Law Commission currently believes that the risks of clarifying the definition of "personal information" by means of official guidance from the Privacy Commissioner outweigh the potential benefits. Otherwise, we have no view at present about how the definition should be clarified, and we welcome suggestions.

Q9 Do the following elements of the definition of "personal information" in the Privacy Act need to be clarified? If so, do you have any suggestions about how this should be done?

- "information"
- "about"
- "identifiable"

Q10 Are there any other issues you would like to raise about the definition of "personal information"?

Human tissue samples and personal information

3.32 There is no reference to human tissue or bodily samples in the Privacy Act, but the definition of "health information" in the Health Information Privacy Code 1994 (HIPC) includes:[169]

> information provided by [an identifiable] individual in connection with the donation, by that individual, of any body part or any bodily substance of that individual or derived from the testing or examination of any body part, or any bodily substance of that individual.

There are similar provisions in the definition of "health information" in section 22B of the Health Act 1956. It is clear, therefore, that information derived from human tissue falls within the definition of "health information". Although not specifically referred to in the Act itself, there is no reason to doubt that information derived from human tissue is included in the general definition of "personal information", so long as the information is about an identifiable individual.

3.33 The question of whether human tissue samples themselves can constitute personal information is a quite different matter. It is difficult to see how such samples could be considered to be personal information under the Act as currently worded. The natural and ordinary meaning of "information" does not include bodily tissue. Rather, such tissue is something from which information may be obtained through testing or other means. The use of the word "about" in the definition of personal information may be another clue: we would not normally say "This blood is about Jane", whereas we do say "This information is about Jane". Finally, the reference in the HIPC to information "derived from" the testing or examination of a body part or bodily substance suggests that information is something distinct from the tissue itself. The previous Privacy Commissioner appeared to accept that neither the Privacy Act nor the HIPC apply to bodily samples.[170] This interpretation is consistent with the Article 29 Data Protection Working Party Opinion on the concept of personal data, which specifically states that human tissue samples are sources of data but are not themselves data.[171]

3.34 If human tissue samples are excluded from the definition of personal information, the question then becomes whether they should be expressly included in the definition. It appears that the only jurisdiction that currently makes express provision for bodily samples in privacy legislation is New South Wales.[172] The definition of "personal information" in the Privacy and Personal Information

169 Health Information Privacy Code 1994, cl 4(1)(d).

170 *"Guthrie Tests"* (a report by the Privacy Commissioner following his inquiry into the collection, retention, use and release of newborn metabolic screening test samples, September 2003) 8 (para 6.4).

171 Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 9.

172 An expert on international data protection law, Lee Bygrave, believes the NSW provision to be unique: Lee Bygrave "The Body as Data? Reflections on the Relationship of Data Privacy Law with the Human Body" (speech to international conference on "The Body as Data" organised by the Victorian Privacy Commissioner, Melbourne, 8 September 2003) 3.

Act 1998 (NSW) states that the definition "includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics".[173] According to Privacy NSW, this provision was included in the Act because:[174]

> the former Privacy Committee was acutely aware of concerns regarding a number of issues involving bodily samples in the NSW context, for instance, the non-consensual access to and disclosure of newborn screening cards for forensic testing and law enforcement purposes.

3.35 Bodily samples are not expressly covered by the Privacy Act 1988 (Cth), but the ALRC and the Australian Health Ethics Committee (AHEC) recommended in a 2003 report on the protection of human genetic information that the Act should be amended to include bodily samples of identifiable individuals in the definitions of "personal information" and "health information".[175] This recommendation was rejected by the Australian Government.[176] The key points in the ALRC/AHEC report's argument for bringing bodily samples within the coverage of the Privacy Act were that:[177]

- Bodily samples are closely analogous to other immediate sources of personal information (such as paper or computer records) that are covered by the privacy principles.
- There are significant gaps in the existing legal protections of the privacy of individuals from whom genetic samples are taken.
- These gaps could be filled by applying the privacy principles to bodily samples, and thereby bringing them within the coverage of an established and well-developed regulatory framework.
- No circumstances had been identified in which adverse consequences for existing practices with regard to the collection and handling of bodily samples could result from the proposed change (although it was acknowledged that special provisions would be needed in the Privacy Act to deal with the application of the privacy principles to bodily samples).

3.36 The argument that, while bodily samples are not themselves information, they are "such an immediate source of personal information (a 'virtual medical record') that they demand similar comprehensive privacy protection",[178] is a strong one. Technology has advanced to the level where genetic testing of human tissue samples can be conducted quickly and increasingly cheaply, and can reveal a significant amount of very personal information about individuals. Furthermore, human tissue samples will often be associated with information that clearly does fall within the definition of personal information in the Privacy Act. For example,

---

173 Privacy and Personal Information Act 1998 (NSW), s 4(2). This definition is also included in the Health Records and Information Privacy Act 2002 (NSW), s 5(2).

174 Privacy NSW "Supplementary Submission to the Australian Law Reform Commission/Australian Health Ethics Committee Joint Inquiry into the Protection of Human Genetic Information" (December 2002).

175 Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) 286 (rec 8–2).

176 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 410.

177 Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) ch 8.

178 Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) 286.

the newborn metabolic screening samples ("Guthrie cards") clearly fall within the coverage of the Privacy Act and the HIPC because, while the blood spots themselves are not information, the cards contain personal details relating to the baby, the mother and the lead maternity carer.[179] It could, therefore, be considered to be increasingly artificial to separate the treatment of bodily samples from the treatment of the information derived from them.

3.37 However, while it would clearly be undesirable from a privacy perspective if the collection, retention, use and transfer of human tissue samples were unregulated, the Privacy Act is not necessarily the most appropriate vehicle for such regulation. There is already a considerable body of law governing human tissue, including:

- the tort of trespass to the person and the offence of assault[180] (which protect against the non-consensual taking of samples directly from a person);
- the New Zealand Bill of Rights Act 1990;[181]
- the Human Tissue Act 2008 and regulations made under the Act;
- the Health and Disability Commissioner Act 1994, and the Code of Health and Disability Services Consumers' Rights;[182]
- the Criminal Investigations (Bodily Samples) Act 1995; and
- the Coroners Act 2006.[183]

The Health Act 1956 (section 121A) also makes provision for the making of regulations about the retention of health information and specimens (defined as "bodily sample[s] or tissue sample[s] taken from a person"), although the Health (Retention of Health Information) Regulations 1996 have not been extended to cover specimens so far. In addition, human tissue is governed by research ethics guidelines and requirements for research to be approved by ethics committees.[184]

3.38 This body of law appears to cover at least some of the gaps identified by the ALRC and AHEC in Australia. For example, the Human Tissue Act 2008 specifically provides for the making of regulations with regard to the export and import of human tissue.[185] Moreover, it is difficult to see what benefit there could be in adding the Privacy Act to the already-complex body of law governing

179 *"Guthrie Tests"* (a report by the Privacy Commissioner following his inquiry into the collection, retention, use and release of newborn metabolic screening test samples, September 2003) 3–4. The cards are separated into two parts after they are received at the National Testing Centre. The part that includes the blood spots has only the baby's surname and National Health Index number written on it, but this part of the card also has a bar code which links it to the other half of the card, containing further personal information about the baby, mother and lead maternity carer.

180 Crimes Act 1961, s 196 (common assault).

181 New Zealand Bill of Rights Act, ss 10 (right not to be subject to medical or scientific experimentation), 11 (right to refuse medical treatment), 21 (right to protection against unreasonable search and seizure).

182 See especially the Code of Health and Disability Services Consumers' Rights, rights 7(9) and (10).

183 Coroners Act 2006, ss 47–56.

184 See Ministry of Health *Guidelines for the Use of Human Tissue for Future Unspecified Research Purposes* (Wellington, 2007).

185 Human Tissue Act 2008, ss 66, 75. See Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) 271–272 for discussion of this issue in the Australian context.

human tissue samples. While there may be gaps in the existing law,[186] any such gaps are probably best addressed by amending the other statutes and regulations listed above, rather than by extending the scope of the Privacy Act. Amending the definition of "personal information" to include bodily samples would take the privacy principles beyond the area of informational privacy into bodily privacy. This would be a significant expansion, and should not be undertaken lightly, especially given the body of existing law governing human tissue samples. It is probably more appropriate to continue to restrict the coverage of the privacy principles to information derived from such samples. It should also be noted that there is no restriction on the Privacy Commissioner reporting or commenting on matters relating to human tissue samples or other issues of bodily privacy, although this would change if the Commissioner's functions were to be restricted to informational privacy (see chapter 6). For example, in reports and submissions on the Guthrie cards and on the Criminal Investigations (Bodily Samples) Amendment Bill, the Commissioner has been free to comment on issues regarding the samples themselves as well as associated personal information.

3.39 We propose that there should be no change to the current position with regard to human tissue samples and the definition of personal information. If such samples were to be brought within the coverage of the privacy principles, further consultation and analysis would be needed to decide what other changes would be required to the Act.

Q11 Do you agree that human tissue samples should not be covered by the definition of personal information in the Privacy Act? Why, or why not?

Q12 Is any clarification needed with regard to the coverage by the privacy principles of genetic information or other information derived from bodily samples?

"INDIVIDUAL"

3.40 As mentioned above, personal information is defined in the Privacy Act as "information about an identifiable individual". "Individual" is defined as "a natural person, other than a deceased natural person". Thus, the definition of individual excludes artificial legal persons (such as companies) or other collective entities, and deceased persons (with some exceptions, discussed below), and consequently information about such persons is excluded from the definition of personal information. The question is whether these exclusions should continue in their current form, be modified, or be removed.

3.41 In considering this question, it is important to note that the answer with respect to the Privacy Act need not be the same as with respect to the tort.[187] There are several reasons for this:

186 See Katie Elkin "The New Regulation of Non-Consensual Genetic Analysis in New Zealand" (2008) 16 JLM 246.

187 The application of the privacy tort to corporations and deceased persons is discussed in New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2009) 152–154; New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, Wellington, 2010) 117–118.

- While the privacy tort is commonly said to protect human dignity, the Privacy Act clearly protects a wider range of interests, including financial interests.
- The Privacy Act protects a broad category of "personal information", rather than the narrower category of "information in respect of which there is a reasonable expectation of privacy" protected by the tort.
- The Privacy Act has greater scope than the tort for partial or modified application to collective entities and deceased persons, such as applying only some privacy principles to them, applying certain principles only to particular sectors by means of a code, or applying the principles to deceased persons only for a specified period of time after death.

Thus, any decision to include collective entities or deceased persons in the coverage of the Privacy Act should not necessarily influence decisions about the application of the privacy tort, or vice versa.

3.42 Any change to the definition of "individual" would affect the Broadcasting Act, which defines "individual" as having the same meaning as in the Privacy Act.[188]

Deceased persons

3.43 While deceased persons are generally excluded from the coverage of the Privacy Act, there are three ways in which information about the deceased does come within the scope of the Act. First, the definition of "personal information" includes "information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act". Secondly, an agency may refuse to disclose information requested pursuant to principle 6 if the disclosure "would involve the unwarranted disclosure of the affairs of another individual *or of a deceased individual*".[189] Thirdly, the Act provides that, for the purposes of the issuing of codes of practice relating to health information, principle 11 (disclosure) shall be read as if it applies in respect of any individual, whether living or deceased.[190] Accordingly, the HIPC provides that rule 11 of the Code applies to health information about the deceased for a period of 20 years after death.[191]

Existing provisions relating to deceased persons in the Privacy Act

3.44 Several people with extensive knowledge and experience of the Privacy Act have told the Law Commission that the Act needs to be more consistent in its application to deceased persons.[192] The first question, therefore, is whether the existing exceptions to the general rule that the Act does not apply to the deceased are appropriate.

188 Broadcasting Act 1989, s 2(1).

189 Privacy Act 1993, s 29(1)(a) (emphasis added).

190 Privacy Act 1993, s 46(6).

191 Health Information Privacy Code 1994, rule 11(5) and (6). However, health information regarding the deceased may be disclosed if the disclosure is to, or is authorised by, the deceased individual's representative; or if the information concerns only the fact of death and the disclosure is by a health practitioner or other authorised person to the deceased person's representative or certain other specified persons: rule 11(1)(a), (b) and (f).

192 Law Commission meeting with people with specialist knowledge of the Privacy Act, 8 May 2008.

Deaths register

3.45 It appears that information about a death maintained pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995 (BDMRRA) was included in the definition of personal information in order to ensure that this information was covered by the public register and information matching controls in the Privacy Act.[193] However, there is no available information about why it was considered desirable that information on the death register should be covered by these controls. It is notable that no similar provision applies to the registers of burials and cremations maintained by local authorities under the Burial and Cremation Act 1964, even though these registers contain names, birth dates and death dates. Information in the burials and cremations registers is not covered by the Privacy Act because it relates to deceased individuals.[194]

3.46 Information from the Department of Internal Affairs suggests that the main reasons for extending privacy protection to the deaths register (using the term "deaths register" loosely to include all the various forms in which the Registrar-General maintains information about deaths under the BDMRRA) are that:[195]

- the deaths register includes information about persons other than the individual who has died, and some of these individuals may still be living;[196]
- the cause of death is recorded on the register, and there may be particular sensitivities in relation to this (for example, if the death was due to suicide or a socially-embarrassing disease); and
- there is a danger that information from the deaths register may be used to engage in identity crime.

3.47 With regard to the first of these points, any information about living individuals contained in the deaths register would be covered by the definition of "personal information" regardless of the specific provision relating to information about a death maintained pursuant to the BDMRRA. This is a good reason for applying privacy protections to the register, but not for including information about deceased persons themselves in the definition of personal information. The second point has some validity, especially given that information about the cause of death will commonly be health information that would be protected against disclosure for 20 years after death under the Health Information Privacy Code. The third point is also persuasive to some extent, although the Department of Internal Affairs acknowledges that restricting access to the BDM register will only go some way towards dealing with the problem of identity crime.[197]

193 *Necessary and Desirable* 49.

194 New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008) 27–28.

195 Department of Internal Affairs "Review of Public Access to Registers Held in the Citizenship Office and Registry of Birth, Death, and Marriages" (May 2005) paras 26–27, 32–34, 38, 119; Law Commission meeting with Department of Internal Affairs regarding the Births, Deaths, Marriages and Relationships Registration Amendment Bill, 5 March 2007.

196 The Births, Deaths, Marriages, and Relationships Registration (Prescribed Information) Regulations 1995, reg 7, provides that death certificates shall contain information about the deceased's parents, partners, children, and the doctor who certified the death.

197 Department of Internal Affairs "Review of Public Access to Registers Held in the Citizenship Office and Registry of Birth, Death, and Marriages" (May 2005) para 33.

3.48 However, while there may be good reasons to apply some controls to the handling of information on the deaths register, this does not mean that the best way of doing so is to include information about deaths maintained under the BDMRRA in the definition of personal information in the Privacy Act. There are a range of controls on information held on the deaths register in the BDMRRA itself, and this would seem to be the most appropriate way of providing appropriately-targeted protection for information about deceased persons contained in the deaths register. If the Privacy Act were no longer to apply to information about deaths held on the deaths register, some amendments to the BDMRRA might be required.

3.49 The question of controls on information matching involving the deaths register is more complex.[198] Section 78A of the BDMRRA authorises the disclosure of deaths information (as well as other information governed by the Act) to certain specified agencies for specified purposes.[199] As at 30 June 2009, eight authorised information-matching programmes involving BDM deaths information were operating.[200] The purposes for which the information is used include detecting benefit fraud, discontinuing benefits to deceased persons, detecting fraudulent passport applications, and cancelling driver licence records relating to deceased persons.[201]

3.50 A deceased person cannot be affected by "adverse action" such as discontinuing benefits, but information-matching programmes involving deaths information could affect living persons if the programme results in a false match.[202] Because of the possible impact on living persons, we believe that data matching involving information from the deaths register should continue to be covered by the information-matching provisions of the Privacy Act.

3.51 We note that information from the deaths register is sometimes matched with information held by agencies in the private sector. For example, the New Zealand Marketing Association has an agreement with the Department of Internal Affairs which permits information from the deaths index to be used in order to remove deceased persons from mailing lists.[203] The information matching provisions of the Privacy Act do not cover information matching between the public and

198 See also the general discussion of information matching in chapter 9.

199 The specified agencies and purposes are listed in Schedule 1A to the BDMRRA. Information matching involving deaths information is subject to the Registrar-General entering into an agreement with the chief executive of the specified agency; the agreement being limited to a purpose listed in Schedule 1A; and the agreement being an information-matching agreement that complies with the Privacy Act. See Department of Internal Affairs "Identity Services Privacy Notice" www.dia.govt.nz (accessed 15 January 2010).

200 Office of the Privacy Commissioner "List of Statutes and Authorised Information Matching Programmes in Operation" (as at 30 June 2009) on "Data Matching – Operating Programmes" page of the OPC website www.privacy.org.nz (accessed 15 January 2010). In addition, disclosure by the Registrar-General of deaths information is authorised by certain other statutes, most notably the Electoral Act 1993: Department of Internal Affairs "Identity Services Privacy Notice" www.dia.govt.nz (accessed 15 January 2010).

201 The information matching programmes involving BDM deaths information are described in *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2009* (Office of the Privacy Commissioner, Wellington, 2009) 50, 54–55, 65, 66–68, 79–80.

202 For example, between 2004 and 2008 there were 17 challenges to notices of adverse action under the Ministry of Social Development's deceased persons data-matching programme, and seven of these challenges were successful: *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2008* (Office of the Privacy Commissioner, Wellington, 2008) 56. There were no challenges under this programme in 2008/09.

203 New Zealand Marketing Association "Launching the Upgrade of the Do Not Mail/Do Not Call Service" (June 2009) www.marketing.org.nz (accessed 15 January 2010).

private sectors. Therefore, if the definition of personal information were no longer to include information on the deaths register, use of such information by the private sector would be governed solely by the provisions of the BDMRRA.

3.52 Our proposals concerning the Privacy Act and information about deaths maintained by the Registrar-General pursuant to the BDMRRA are as follows:

- consultation should be undertaken with the Department of Internal Affairs and the Registrar-General to determine what amendments, if any, might be required to the BDMRRA if the Privacy Act's coverage of deaths information were to end;
- the existing provision in the definition of "personal information" should be deleted, subject to any necessary amendments to the BDMRRA being enacted, meaning that for most purposes information about deceased persons on the deaths register will not be covered by the Privacy Act;
- specific provision should be made in the Privacy Act (or a new Data Matching Act, as proposed in chapter 9) for the application of the information-matching section of the Act to deaths information.

Ground for refusal of access

3.53 The provision in section 29(1)(a) of the Privacy Act, which allows an agency to refuse access to information requested under principle 6 if it would involve the unwarranted disclosure of the affairs of another individual, whether living or deceased, is based on grounds under the OIA and the Local Government Official Information and Meetings Act 1987.[204] Chapter 11 raises the question of whether there should be greater consistency between the privacy terminology in the OIA and the Privacy Act, and this includes the question of whether the withholding ground in section 9(2)(a) of the OIA should continue to protect the privacy of the deceased. However, even if the OIA withholding ground continues to refer to the privacy of deceased persons, there could be a case for removing or narrowing the reference to deceased persons in section 29(1)(a) of the Privacy Act. The scope of OIA requests is potentially much wider than that of Privacy Act access requests, with greater potential to reveal information about deceased persons that they and their families might reasonably have expected would not be made public. It is also arguable that people's right of access to information about themselves is stronger than their right of access to official information, and furthermore that any information about deceased persons released in response to an access request must, in some sense, also be information relating to the requester.

3.54 There do not appear to be any Privacy Commissioner case notes or Tribunal cases that consider the application of section 29(1)(a) to deceased persons. There have been a number of Ombudsmen decisions concerning whether information about deceased persons should be withheld under section 9(2)(a) of the OIA.[205] These decisions, made in consultation with the Privacy Commissioner, seem to

204 Official Information Act 1982, ss 9(2)(a), 27(1)(b); Local Government Official Information and Meetings Act 1987, ss 7(2)(a), 26(1)(b).

205 See for example Case W31776 in *11th Compendium of Case Notes of the Ombudsmen* (Butterworths, Wellington, 1998) 95; Cases A6553, A6580, A6722, W41406, W42031 in *12th Compendium of Case Notes of the Ombudsmen* (Office of the Ombudsmen, Wellington, 2000) 89–95, 97–99.

depend very much on the particular facts of the case. It is noticeable in the OIA cases that the requesters were specifically seeking information about the deceased persons in question, rather than seeking a wider body of information of which the deceased person's information simply formed part. In most cases, the requesters were family members of the deceased person. The Ombudsmen's Practice Guidelines for Official Information provide little guidance about the withholding of information on deceased persons.[206]

3.55 We believe that the protection of information relating to deceased persons in section 29 of the Privacy Act is too broad, and should be more consistent with the protection in the rest of the Act. We propose that:

- the words "or of a deceased individual" should be deleted in section 29(1)(a); and
- a new withholding ground should be added to section 29, dealing with situations where the disclosure of the information would involve the disclosure of health information about a deceased person.[207]

3.56 We suggest that the new withholding ground should be broadly consistent with the restrictions on disclosure of health information about deceased persons in rule 11 of the HIPC. That is, it should apply to "health information" as defined in the HIPC for up to 20 years after death, and access should be allowed if the person making the request is the deceased's personal representative or is authorised by the deceased's personal representative. However, in contrast to the HIPC, the withholding ground should not be limited to health information held by a "health agency".

3.57 If any additional protections for information relating to deceased individuals, such as a broader power for the Privacy Commissioner to make provision for information about deceased persons in codes of practice (see below), were to be included in the Privacy Act, further targeted withholding grounds might be needed.

Health information

3.58 Section 46(6) of the Privacy Act, which provides for the application of the disclosure principle to deceased persons for the purposes of any privacy code of practice relating to health information, was introduced by the select committee considering the Privacy of Information Bill. The select committee decided that it was necessary to provide some protection for the medical records of deceased persons, given the sensitive nature of such records and the fact that medical confidentiality has traditionally extended beyond a patient's death.[208]

3.59 This provision, and the provisions relating to disclosure of health information about deceased persons in the HIPC, seem to us to be appropriate means of providing protection for information about deceased individuals in the health

206 Office of the Ombudsmen *Practice Guidelines: Official Information* available at www.ombudsmen.govt.nz – see Part B, ch 4.1, 5, and Part E, 4, for brief references to information about deceased persons.

207 One overseas statute (albeit a freedom of information rather than an information privacy statute) that has a specific withholding ground for a deceased person's health information is the Freedom of Information (Scotland) Act 2002, s 38(1)(d).

208 *Necessary and Desirable* 210.

context. We propose below that the Privacy Commissioner's power to apply codes of practice to information about deceased individuals should be extended. If the Commissioner does not get a general power to make codes covering information about the deceased, however, consideration should be given to the Privacy Commissioner's recommendations for specific amendments to section 46(6).[209]

Q13 Should there be any changes to the existing provisions relating to deceased persons in the Privacy Act? (See in particular the proposals in paragraphs 3.52 and 3.55.)

Possible new provisions

3.60 The discussion above concerns the existing provisions of the Privacy Act in relation to deceased individuals. We now consider whether any additional provisions in relation to information about deceased individuals are needed. A number of information privacy statutes in Australian states and territories cover personal information about individuals who have been dead for not more than specified periods of time (the longest of which is 30 years).[210] The ALRC has recommended that the Privacy Act 1988 (Cth) should be amended to include specific provisions dealing with the personal information of individuals who have been dead for 30 years or less, where the information is held by an "organisation" (that is, by a private sector body). These provisions should relate to the use and disclosure, access, data quality and data security principles under the Act.[211] The Australian Government has rejected this recommendation, although its main reason for doing so appears to be that there are constitutional limitations on the Federal Government's power to legislate in this area.[212]

3.61 Arguments for extending the Privacy Act's coverage of information about deceased individuals include:

- People may be reluctant to provide agencies with their personal information while they are alive if they believe that it can be disclosed immediately after their deaths.
- The families of deceased individuals have an interest in how such individuals' personal information is handled. They can suffer distress if intimate information about their deceased relatives is disclosed.
- The idea that deceased persons have no privacy interest may be specific to Pākehā culture, and may not be shared by other cultures.
- Duties of confidence, which overlap with privacy, can survive death.
- Some statutes recognise privacy interests of deceased persons, as discussed further below.

209 *Necessary and Desirable* 210–211, rec 75; *1st supplement to Necessary and Desirable* 13–14, rec 75A.

210 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 359–360.

211 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 8–1 and ch 8 generally. The ALRC recommended that information about deceased individuals held by "agencies" (public sector bodies) should continue to be regulated by the Freedom of Information Act 1982 (Cth) and the Archives Act 1983 (Cth): ibid, 369.

212 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 28.

3.62 Arguments against include:

- Privacy is a human right which is inherently personal, and therefore the right of privacy dies with the person.
- The deceased cannot suffer humiliation, loss of dignity, financial loss, threats to physical safety, or any of the other harms that privacy law is intended to protect against.
- The tort of defamation, which is closely related to privacy, does not survive death.
- Applying the Privacy Act to information about deceased persons would be fraught with practical difficulties. In particular, it would be difficult to apply the concept of consent, and to decide how the right of access under principle 6 would apply.

3.63 There is little information available about public attitudes to protection of personal information about deceased individuals. However, a survey conducted for Statistics New Zealand in 2005 found that 26 per cent of respondents would be concerned if all census forms were to be stored with names and addresses attached and then released after 100 years to statistical researchers only. Thirteen per cent of respondents would be "very concerned" (10 on a scale of 0 to 10).[213] Although the majority of respondents were not concerned, it is notable that such a significant minority objected to the release of their information even though they would almost certainly be dead and even if it was to be used only for statistical research. Different cultural perspectives also need to be taken into account. In particular, there is some evidence that Māori beliefs may recognise a right to protection of deceased individuals' privacy and reputation.[214]

3.64 Some other statutes already recognise the privacy of information about deceased persons to some degree. The explicit reference to the privacy of deceased persons in the OIA has already been mentioned.[215] The Coroners Act 2006 also provides (based on a recommendation by the Law Commission) for coroners to prohibit publication of evidence or submissions to protect "personal privacy".[216] This does not expressly include the privacy of deceased persons, but nor does it exclude it.[217] The New Zealand Public Health and Disability Act 2000 includes restrictions on the disclosure by mortality review committees appointed under the Act of information that became known to a person only because of the committee's functions being carried out, along with penalties for breach of these

213 *Public Attitudes to the Confidentiality, Privacy and Security of Official Government Survey Data* (survey conducted by UMR Research for Statistics New Zealand, May 2005) 86. The survey was of a nationally-representative sample of 1000 New Zealanders aged 18 and older.

214 Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press/BSA, Wellington, 2004) 57; Carol Archie *Pou Kōrero: A Journalists' Guide to Māori and Current Affairs* (New Zealand Journalists Training Organisation, Wellington, 2007) 87; *Turia v TVNZ* (9 November 2000) Broadcasting Standards Authority 2000–165.

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

216 Coroners Act 2006, s 74; New Zealand Law Commission *Coroners* (NZLC R62, Wellington, 2000) 123–124

217 In *Re an inquest into the death of JRF Fardell* (1 November 2006) HC AK CIV 2006-404-3638, para 59, Heath J ruled that "the privacy interests of the deceased and his family" justified a limited suppression order. Although the Coroners Act 2006 was not yet in force, Heath J commented (para 65) that his views on the nature of the discretion to withhold information under the 1988 Act would be equally applicable to section 74 of the new Act.

restrictions.[218] The information handled by mortality review committees will mainly be information about deceased persons, and it is clear that the intention is that such information should be treated as strictly confidential.[219]

Options for recognising privacy of information about deceased persons

3.65 If it is considered desirable to make additional provision in the Act for information about the deceased, there are a number of ways in which this could be done:

- amending the definition of "individual" so that the Privacy Act as a whole applies to information about deceased persons for a specified period after death;
- introducing a new part of the Act making specific provision for the ways in which some of the privacy principles should apply to information about deceased persons;
- providing that codes of practice made under the Act can apply to deceased persons; and
- introducing targeted provisions to deal with specific issues concerning information relating to deceased individuals.

3.66 The first option, applying the Privacy Act as a whole to information about deceased persons for a specified period after death, seems too sweeping. There would be major problems about how to apply the privacy principles to information about deceased persons, and amendments to the privacy principles would undoubtedly be required. The second option, which is essentially what the ALRC has recommended, is better. It would mean that only some principles could be applied to deceased persons' information, and that specific provision could be made as to how these principles would apply. Even so, it would be difficult to come up with provisions that would be suitable for all contexts. New Zealand's Privacy Act has the advantage of making provision for the creation of codes of practice to deal with the application of the Act to particular sectors. We consider that this would provide greater flexibility and scope to tailor provisions relating to deceased persons to particular contexts.

Codes of practice

3.67 At present, section 46(6) makes very limited provision for the application of a code of practice to information about deceased persons. Section 46(6) deals only with codes of practice relating to health information, and only with principle 11 (disclosure). Disclosure of health information about the deceased is, indeed, a sensitive matter, and it seems appropriate that it should be regulated for 20 years after death. However, other principles may also be applicable to deceased persons' health information. For example, the Privacy Commissioner has recommended

218 New Zealand Public Health and Disability Act 2000, s 18(7); sch 5, cls 3–6.

219 Perinatal and Maternal Mortality Review Committee "About Us: Privacy of PMMRC Information" www.pmmrc.health.govt.nz (accessed 9 September 2009); Child and Youth Mortality Review Committee "About Us: Privacy of CYMRC Information" www.cymrc.health.govt.nz (accessed 9 September 2009). However, the relevant provisions in the Act are limited to information that is personal information within the meaning of section 2(1) of the Privacy Act: New Zealand Public Health and Disability Act 2000, sch 5, cl 3(a). This means that the provisions do not in fact apply to information about deceased persons except for information about deaths contained in the deaths register.

that principle 5 (security) should apply to such information.[220] Furthermore, there may be contexts other than the health sector in which it would be appropriate to make provision for information relating to deceased persons. One example could be the banking sector. In a letter to the Law Commission, the New Zealand Bankers' Association raised the issue of disclosure of information about deceased customers' accounts. They noted that bankers' common law duty of confidentiality probably continues after death, and that:[221]

> Front line staff often experience pressure from relatives of deceased people to provide information about the deceased person's accounts. Some banks consider it appropriate to deal only with the executors of the estates to avoid disputes. Bank staff come under a lot of pressure to disclose information to relatives so clarifying the law in this area would be beneficial.

The Australian Bankers' Association similarly submitted to the ALRC that, as far as possible, banks handle the personal information of deceased individuals in the same way as that of living individuals, and that both should be regulated in the same way.[222] Banking would seem, therefore, to be an industry in which it might be appropriate to extend the coverage of the privacy principles to information about deceased persons by means of a code of practice.

3.68 There seems to be no good reason why the application of codes of practice to information about the deceased should be limited to disclosure of health information. There would seem to be a good case for allowing the Privacy Commissioner to apply any of the principles to information about deceased persons in any code of practice that she develops. To be clear, we do not have in mind a generic code of practice relating to information about the deceased. Rather, we propose that codes of practice dealing with particular sectors should be able to apply the principles to information about deceased persons, as the HIPC already does with respect to disclosure of health information.

3.69 It could be objected that this gives the Commissioner the power to amend the application of the Act in a very significant way. However, the Act already contains a number of procedural safeguards in relation to codes of practice, and we are proposing to add the additional safeguard of approval by Cabinet. We do not believe that the Commissioner would lightly take the step of applying the principles to information about the deceased, or that such a significant step would fail to be fully debated at several stages in the process.

3.70 Our preliminary view is that the Act should be amended to allow codes of practice to be applied to information about deceased persons. We are not inclined to extend the Act's coverage of information about the deceased in any other way.

220 *1st supplement to Necessary and Desirable*, rec 75A.

221 New Zealand Bankers' Association to the Law Commission (21 July 2008) Letter.

222 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 366.

Q14 We propose that the Privacy Act should be amended to allow codes of practice to apply any of the privacy principles to information about deceased persons. Do you agree?

Q15 Should any other amendments be made to the Privacy Act to extend its application to information about deceased persons?

Survival of Privacy Act complaints after death

3.71 Another question concerns complaints made by a person who dies before the complaints process has been completed. This issue arose in the case of *Yakas v Kaipara District Council*. In that case, the complainant died after the Privacy Commissioner's investigation had been completed, but before proceedings could be continued in the Tribunal. The complainant's son sought to continue proceedings on his mother's behalf, claiming that the notice of intention to bring proceedings was signed by his mother before her death. There was some uncertainty, however, about when the notice was in fact signed, and the Tribunal had no evidence that the complainant's son was the legal administrator of his mother's estate. The Tribunal did not accept that proceedings could be considered to have commenced while the complainant was still alive. It accepted the defendant's submission that, as the plaintiff was not alive when the claim was commenced, the claim was not brought by an "aggrieved individual" in terms of section 83 of the Privacy Act, and therefore the Tribunal had no jurisdiction to deal with it. The Tribunal noted that the definition of "individual" in the Act excluded deceased natural persons, and that:[223]

> In our view the defendant is right to say that section 83 limits the right to bring proceedings in the Tribunal to "aggrieved individuals" in such a way as to ensure that proceedings are brought by individuals on their own account, and that the right to bring proceedings exists only for those individuals who are alive at the time the proceedings are commenced.

As a result, the Tribunal did not need to consider the defendant's alternative submission, that any cause of action the plaintiff may have had under the Act could not be pursued by her estate after her death.

3.72 Paul Roth has questioned the Tribunal's interpretation of the Act in *Yakas*. The Tribunal seemed to rely not only on the definition of "individual" but also on the provision in section 83 that the aggrieved individual "may himself or herself" bring proceedings before the Tribunal. Roth suggests that, rather than requiring that an individual personally bring proceedings on his or her own account, this provision in section 83 can be seen as standing in contrast to the position in section 82(2), which refers to the bringing of proceedings by the Director of Human Rights Proceedings. If this interpretation is accepted, Roth argues: [224]

> then the words no longer suggest that proceedings may only be brought personally by living individuals, but might also be brought on behalf of individuals who were alive when the cause of action under the Privacy Act accrued.

223 *Yakas v Kaipara District Council* [2004] NZHRRT 10, para 11.

224 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA83.4(c), 503,214.

3.73 Whatever the correct legal position with regard to the current provisions of the Act and the particular facts of *Yakas*, it seems wrong in principle (as Roth also argues) "that causes of action under the Privacy Act should be barred by death, and that the 'aggrieved individual' cannot be represented, after death, by the executor or administrator of his or her estate".[225] Section 3(1) of the Law Reform Act 1936 provides that, on the death of any person, all causes of action (apart from defamation) vested in the deceased person shall survive for the benefit of his or her estate. In principle, Privacy Act proceedings in the Tribunal under section 83 should be covered by this provision in the Law Reform Act, and if a contrary intention is suggested by the wording of section 83 this should probably be amended. Roth makes the point that, if causes of action under the Privacy Act are rendered void by death, this could create an incentive for respondents to be obstructive so as to delay the Commissioner's investigations in the hope that the complainant will die before the matter is resolved. Proceedings brought by the Director of Human Rights Proceedings under section 82 (which may in future be brought by the Privacy Commissioner under our proposals in chapter 8) are probably a different matter. Comments by the Court of Appeal in a case relating to the Health and Disability Commissioner Act suggest that a case brought by the Director may not be a "cause of action" in terms of section 3(1) of the Law Reform Act 1936.[226]

3.74 The question of what should happen when a complainant dies while a complaint is still at the stage of mediation or investigation by the Privacy Commissioner is perhaps less clear. At this stage, the complaint is probably not a "cause of action" that would be covered by the Law Reform Act 1936. There is probably no reason why the Commissioner cannot continue mediation with the executor or administrator of the deceased's estate, or with a person or persons nominated by the deceased prior to death to represent him or her, if the respondent agrees. However, if the respondent does not agree to such a process, or if the parties are unable to reach an agreed settlement, it is unclear how the Commissioner should proceed. Certainly, the Commissioner has discretion under section 71(2) of the Act to take no further action if it appears that, "having regard to all the circumstances of the case, any further action is unnecessary or inappropriate". Normally, where the Commissioner has decided that a complaint ought not to be proceeded with, the complainant has a right under section 83 to bring proceedings before the Tribunal. Does the Commissioner's decision to take no further action on a complaint give rise to a "cause of action" that can then be pursued by the deceased's representatives? At what point, precisely, does a cause of action accrue? On the other hand, if the Commissioner considers that further action is appropriate (perhaps because the complaint reveals wider systemic problems), can an investigation be continued despite the complainant's death?

3.75 We propose that the Privacy Act should be amended to make clear that section 3(1) of the Law Reform Act 1936 applies to causes of action under the Privacy Act.

225 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA83.4(c), 503,214.

226 *Marks v Director of Health and Disability Proceedings* [2009] NZCA 151, para 65 Glazebrook J.

Q16 We propose that the Privacy Act should be amended to make clear that section 3(1) of the Law Reform Act 1936 applies to causes of action under the Privacy Act. Do you agree? Do you have any other suggestions about survival of Privacy Act complaints after death?

Legal persons and groups

3.76 Section 29 of the Interpretation Act 1999 defines "person" as including "a corporation sole, a body corporate, and an unincorporated body". By consistently using the term "individual" rather than "person", and by limiting the meaning of "individual" to natural persons, the drafters of the Privacy Act ensured that it would not apply to the handling of information relating to corporations or unincorporated groups. Unlike the exclusion of information about deceased persons, there are currently no exceptions to the exclusion of information about legal persons and other collective entities.

3.77 There is limited recognition of the privacy interests of corporations in other legislation. The OIA defines person as including "a corporation sole, and also a body of persons, whether corporate or unincorporated".[227] Sections 24 to 27 of the OIA provide for rights of access to and correction of official information about an identifiable person. These provisions originally applied to both natural and legal persons, but following the enactment of the Privacy Act the OIA provisions were amended so that they now confer access and correction rights only on bodies corporate.[228] It is also worth noting that section 29 of the New Zealand Bill of Rights Act 1990 provides that the provisions of the Bill of Rights apply, "so far as practicable", for the benefit of legal persons. This means, among other things, that legal persons can benefit from the protection of privacy in section 21 of the Bill of Rights Act: protection against unreasonable search and seizure.

3.78 The OECD Privacy Guidelines, with which the Privacy Act is said to be "in general accordance" (Long Title to the Act), do not deal with information relating to legal persons or groups.[229] They define "personal data" as information relating to an identified or identifiable "individual".[230] The Expert Group established to develop the Guidelines specifically considered whether the Guidelines should cover legal persons and groups, but no consensus could be reached on this issue. However, the Guidelines only establish minimum standards for domestic legislation, and there is nothing to prevent member countries from developing data protection laws and policies for corporations and groups.[231] Most personal data protection statutes in other jurisdictions apply only to information about natural persons, but a small number of countries also apply data protection

227 Official Information Act 1982, s 2(1).

228 Official Information Act 1982, s 24(2).

229 For a comprehensive, comparative survey of issues relating to data protection rights for private collective entities see Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) chs 9–16.

230 Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), para 1(b).

231 Explanatory Memorandum to the OECD Privacy Guidelines, paras 19(c), 31–33, 49.

laws to information about legal persons, at least to some extent.[232] In line with the recommendation of the South African Law Reform Commission, the Protection of Personal Information Bill recently introduced in South Africa provides that "personal information" can, "where it is applicable", include information about a "juristic person".[233] By contrast, the ALRC recommended that the Privacy Act 1988 (Cth) should not be amended to cover information about corporations or groups.[234]

3.79 We do not favour extending the Privacy Act to cover corporations. We believe that such an extension is inconsistent with the purpose of the Act, which is "to promote and protect *individual* privacy"[235] in accordance with the OECD Guidelines and with international human rights law. Privacy is a human right, based ultimately on protection of individual dignity, and the harms that can be suffered by corporations through misuse of their information are fundamentally different from those which can be suffered by individuals. The interests of corporations that are akin to privacy are adequately protected by other areas of law, including breach of confidence, defamation, intellectual property, and laws criminalising various forms of surveillance, computer hacking, and theft of information. Furthermore, corporations are inherently public bodies which take on obligations of transparency in return for the protections that come with their legal status. They do not have the same rights as individuals to keep their information private (although, as noted, they can protect some kinds of information through other branches of law). Extending the Privacy Act to cover corporations would also give rise to uncertainty and practical difficulties about the application of the privacy principles, and would add to compliance costs.

3.80 While we do not favour giving corporations rights under the Privacy Act, we invite submissions on the specific question of whether corporations should have rights of access or correction under principles 6 and 7. Gehan Gunasekara from the University of Auckland has proposed that, at a minimum, corporations should be given access and correction rights, which would be consistent with the rights that they already possess with respect to official information.[236] There is a danger, however, that if access rights were to be extended to corporations, they could be used by companies to gather intelligence about the information held about them by their competitors. This could include information about their competitors' attitudes towards them and business strategies for competing with them. This objection would not apply if access and correction rights were limited to the field of credit reporting. Several Scandinavian countries that do not make

232 Argentina, Austria, Denmark, Iceland, Italy, Luxembourg, Norway and Switzerland have enacted data protection legislation expressly covering legal persons or other collective entities. However, in 2000 Demark, Iceland and Norway either abolished or reduced the coverage of data relating to legal persons in their data protection laws. Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 178–179, 195; Personal Data Protection Act of 2000 (Argentina), s 2.

233 Protection of Personal Information Bill (South Africa), B 9-2009, cl 1; South African Law Reform Commission *Privacy and Data Protection: Report* (SALRC Project 124, Pretoria, 2009) 72–84.

234 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) ch 7.

235 Long Title to the Privacy Act 1993 (emphasis added).

236 Gehan Gunasekara "Privacy Rights for Companies?" [2008] NZLJ 30.

general provision for information about corporations in their data protection laws do, however, provide for rights of corporations with respect to information held about them by credit reporting companies.[237] Gunasekara argues that:[238]

> In a credit-driven economy, accurate credit reporting and the right to verify and correct inaccurate statements are invaluable. Accurate reporting is just as important to companies whose credit-worthiness is their most important asset. It is difficult to see what justification exists to deny companies the same rights as natural persons in this area.

There is at least an arguable case, therefore, for providing in the Act that any code relating to credit reporting may provide for access and correction rights for corporations.

3.81 The question of whether the Privacy Act should apply to unincorporated groups is somewhat different from the question of its application to legal persons.[239] The idea of collective privacy or group rights to privacy has been raised, particularly in relation to information about Māori and other indigenous peoples,[240] but it is hard to see how it could work in practice. The Privacy Act is based on each individual's rights to control information relating to that individual, and it is very difficult to see how it could apply to groups without legal personality. Unincorporated bodies, such as sporting clubs or Māori tribes that do not have a legal identity recognised under statute, cannot sue in tort. They may, however, have common interests that the law could recognise. We suggest that the best way of doing so would be by making better provision in the Privacy Act for representative complaints, as discussed in chapter 8.

Q17 Should the Act provide that any code of practice relating to the credit reporting industry may provide for access and correction rights for corporations? Should the Act provide generally for access and correction rights for corporations?

Can information about a corporation be information about an individual?

3.82 The issue of whether, in some circumstances, information about a corporation can be information about the person or persons behind that corporation, came up in a Complaints Review Tribunal case, *C v ASB Bank*. C was the sole director and owner of all but one share in a business, and he used the company's bank account for personal as well as business transactions. After he and his wife separated, his wife obtained copies of the company's bank statements from the bank.

237 Denmark's data protection law applies to corporations in respect of information held about them by credit reporting agencies; Sweden provides in its Credit Reporting Act for access and correction rights of corporations in relation to information held by credit reporting agencies; and Norway's data protection law allowed (as of 2002) for the future introduction of protection for legal persons with respect to credit reporting information: Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 195, 202, 206.

238 Gehan Gunasekara "Privacy Rights for Companies?" [2008] NZLJ 30, 30.

239 See Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) ch 15.

240 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 106–107; Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 339–351.

C complained about this unauthorised disclosure by the bank, and submitted to the Tribunal that the bank statements were personal information. He argued that "information which appears on its face to be information about a company rather than an identifiable individual can be transformed into personal information" by factors such as the nature of the company (the fact that it was a one-person operation); the fact that the account was used in part for personal transactions; the purpose for which his wife obtained the information (she was interested in information about him, not about the company); and the use to which the information was put (the fact that it was combined with other information about him held by his wife and used to draw conclusions about him). The Tribunal agreed with the defendant bank's submission that the information was about the company, not about C, and was therefore outside the scope of the Privacy Act. In the Tribunal's view, it could not find otherwise without lifting the corporate veil and disregarding a century of company law.[241]

3.83 The Tribunal's very strict interpretation in *C v ASB Bank* seems out of character with the spirit and the generally flexible approach of the Privacy Act.[242] In its 1983 report on privacy, the ALRC stated that:[243]

> The creation of a corporate or other business structure for a commercial, family or other purpose should not prevent a claim, in the name of a business association, which is in essence one affecting intimate personal interests of an identifiable private individual. A person should have standing … where he can show that his claim, while nominally concerning an artificial legal person, would affect his personal interests. In other words, [the Privacy Commissioner should] be entitled to pierce the corporate veil and investigate any complaint which, while in appearance one concerning a corporation, was in reality one concerning an individual.

We believe that this is the preferable approach, and that the Privacy Act should be amended to make this clear. To do otherwise is to leave a gap in the Privacy Act's coverage of information that, by any reasonable interpretation, relates to an identifiable individual.[244] However, we recognise that, by "piercing the corporate veil", such a proposal could be seen as "disregard[ing] a hundred years of company law and jurisprudence".[245] We therefore invite submissions on the implications for other areas of law.

3.84 A related question, about which we also seek submissions, concerns the circumstances in which information about a trust can be personal information, and whether the Privacy Act should make provision for information about trusts.

---

241 *C v ASB Bank Ltd* (26 August 1997) Complaints Review Tribunal 21/97.

242 Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 211–212; Paul Roth "What is Personal Information?" (2002) 20 NZULR 40, 57–58.

243 Australian Law Reform Commission *Privacy* (vol 1, ALRC R22, Australian Government Publishing Service, Canberra, 1983) 15.

244 Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 210–215; Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 23–24.

245 *C v ASB Bank Ltd* (26 August 1997) Complaints Review Tribunal 21/97, 4 (quoting the words of counsel for the defendant).

Q18 We propose that the Privacy Act should be amended to make clear that, despite the general exclusion of information about legal persons from the definition of personal information, information about a legal person can be personal information if it is also clearly information about an identifiable individual. Do you agree? Would this have implications for other areas of law?

Q19 Should the Privacy Act be amended to clarify the circumstances in which information about a trust can be personal information?

"COLLECT"

3.85 The definition of "collect" in the Privacy Act states simply that "**Collect** does not include receipt of unsolicited information." The sole purpose of the definition, then, is to provide that unsolicited information will not be "collected" for the purpose of the Act ("the unsolicited information exception"), and therefore will not be covered by the collection principles (principles 1 to 4). The definition of "collect" does not affect the interpretation of the other privacy principles, as principles 5 to 12 do not use the word "collect". Principles 5 to 11 refer to information that an agency "holds", and principles 10 and 11 also refer to the purposes for which information was "obtained". "Obtained" is undefined, but it seems clear that it includes both information that was collected by the agency and information that is held by the agency but was unsolicited. The Act does not define "unsolicited" or "solicit".

3.86 A report to the Minister of Justice on the Privacy of Information Bill suggested definitions of "collect" and "obtain", but these were not included in the Bill.[246] The report defined "collect" as including "solicit, and the taking of any other action by the agency to get personal information into its possession from outside the agency", while "obtain" was defined as including "solicit, collect, and the coming into possession of personal information from outside the agency in any other way".

3.87 It does not seem to be common internationally to define "collect" in information privacy legislation, or to specifically exclude receipt of unsolicited information from the meaning of "collect". However, the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW) both provide that information is not collected for the purposes of the Acts if receipt of that information is unsolicited.[247] In addition, Information Privacy Principles 2 and 3 in the Privacy Act 1988 (Cth) apply only to information that is solicited by the collector.[248] "Solicit" is defined, in relation to personal information, as meaning "request a person to provide that information, or a kind of information in which that information is included."[249] However, the National

246 *Privacy of Information Bill: Directions Report to the Minister of Justice* (23 October 1992), cited in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA2.5, 6.13(b), 201,801, 204,201.

247 Privacy and Personal Information Protection Act 1998 (NSW), s 4(5); Health Records and Information Privacy Act 2002 (NSW), s 10.

248 Privacy Act 1988 (Cth), s 14.

249 Privacy Act 1988 (Cth), s 6(1).

Privacy Principles in the same Act do not distinguish between solicited and unsolicited information. The ALRC's proposed Unified Privacy Principle 2 (Collection) would not exclude unsolicited information from its coverage, but would include special provisions about how unsolicited information should be handled. Essentially, the ALRC recommends that unsolicited information should either be destroyed or, if it is retained, treated in the same way as if it had been actively collected.[250]

3.88 We propose in chapter 4 that privacy principle 2 should be amended to include a provision about the handling of unsolicited information along the lines of the ALRC's recommendation. This proposal can go ahead regardless of whether or not the unsolicited information exception is retained.

3.89 The main difficulty created by the definition of "collect" is the potential for uncertainty about what "unsolicited" means. Some types of information are clearly unsolicited. For example:[251]

- Information about an individual may be provided to an agency by a third party without the agency asking for it (as in the case of a tip-off that a person is engaging in benefit fraud).
- Information may be sent to an agency by mistake (as in the case of misdirected mail, faxes or emails).
- Promotional material containing personal information may be sent to an agency without the agency having invited such material (as in the case of a business flyer which includes names and contact details).

3.90 While the examples just given are reasonably straightforward, there are a number of ways in which the unsolicited information exception may cause uncertainty about the scope of "collection". In particular, Paul Roth has raised the question of whether surveillance by means of a recording or monitoring device is collection for the purposes of the Act. He argues that such surveillance is not collection because information is not solicited in the sense of a request for information being made to a person. This interpretation is not accepted by either the Privacy Commissioner or the Human Rights Review Tribunal, both of which have consistently taken the view that the use of surveillance to obtain information does constitute collection.[252]

3.91 There was limited support for Roth's view in the Court of Appeal decision in *Harder v Proceedings Commissioner*. That case involved two conversations between the complainant and a lawyer, both of which the lawyer recorded without informing the complainant that he was doing so. The first phone call was unsolicited in the sense that it was made by the complainant of her own accord, while the second phone call was solicited in that it had been arranged that the complainant would ring the lawyer back. With respect to the first conversation, the Complaints Review Tribunal concluded that, by switching on the tape recorder, the lawyer had ceased to be a passive recipient of unsolicited

250 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 21-3, 726.

251 Office of the Privacy Commissioner (Federal) *Submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72* (Sydney, 2007) 317.

252 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA2.5, 151,802–151,803.

information and had become an active collector of the information. The Court of Appeal disagreed, holding that "The unsolicited nature of the information was not affected by the fact that it was recorded or the way it was recorded. It was therefore not relevantly collected."[253] It must be emphasised, however, that the question at issue was whether information that was otherwise unsolicited (and therefore not collected) could be transformed into information that was collected by the simple act of recording it. *Harder* is of limited relevance to a situation such as deliberately installing a camera in order to obtain images of people in a particular area.

3.92 Surveillance is not the only area in which the meaning of "unsolicited", and therefore of "collect", may be unclear. Another example concerns agencies, or sections within agencies, that exist in order to receive inquiries or complaints (for example, customer service or complaints departments within commercial enterprises, or complaints bodies such as professional disciplinary tribunals). Do such agencies "solicit" the information that is provided to them? Paul Roth asks:[254]

> Can alerting customers to the existence of such a service, and directing them to it in the case of complaints, mean that the agency concerned is, in a sense, "collecting" such information, or is any information obtained through such channels still "unsolicited"?

This issue has come up in relation to the similar unsolicited information exception in the NSW legislation. In one case, involving disclosure to a doctor who was the subject of a complaint to the NSW Medical Board of information provided as part of that complaint, the Administrative Decisions Tribunal found that the complaint to the Medical Board was unsolicited. The Tribunal commented that "virtually all complaints received by investigative agencies will be unsolicited", although that did not mean that all information provided by complainants to such agencies will be unsolicited.[255] However, Privacy NSW has said that agencies should not treat complaints to them as unsolicited if they hold themselves out as being the appropriate body to receive such complaints.[256]

3.93 A third area of possible uncertainty concerns what could be called "internally-generated information". Examples include:

- The outcome of a completed disciplinary process. In *Boyle v Manurewa RSA Inc*, the Human Rights Review Tribunal found that the outcome of a disciplinary process that had run its course was not information that had been "collected" for the purposes of the Privacy Act.[257]
- Information that is generated automatically in the course of a transaction or similar activity. In a submission to the Privacy Commissioner's *Necessary and Desirable* review, Telecom New Zealand stated that it was unclear whether "collect" included automatically-generated information, such as certain types

253 *Harder v Proceedings Commissioner* [2000] 3 NZLR 80, para 25 (CA) Tipping J.

254 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.5, 151,801.

255 *KD v Registrar, NSW Medical Board* [2004] NSWADT 5, para 27.

256 New South Wales Law Reform Commission *Privacy Legislation in New South Wales* (NSWLRC CP3, Sydney, 2008) 87.

257 *Boyle v Manurewa RSA Inc* [2003] NZHRRT 16, para 31.

of call records about individual subscribers. Telecom considered that the generation of such records should fall within the definition of "collect", and that the definition could be amended to make this clear.[258]

- Information contained in employee emails archived by the employer's computer system. Paul Roth comments that:[259]

> Personal information extracted from a computer that automatically archives or maintains a record of all e-mail messages would presumably constitute the receipt of unsolicited information, as the personal information disclosed in the messages would not have been solicited from the individual concerned… .

3.94 Considering the meanings of "collect", "solicit" and "unsolicited" in ordinary usage is of some assistance. Dictionary definitions of "collect" include "bring or come together; assemble, accumulate"; "systematically seek and acquire (books, stamps, etc.), esp. as a continuing hobby"; "obtain (taxes, contributions, etc.) from a number of people"; "call for; fetch; obtain or gather (*went to collect the laundry*)"; and "infer, gather, conclude".[260] These definitions tend to suggest that collection involves making some effort to acquire something, and especially that to collect something is to acquire it or bring specimens of it together systematically or purposefully. The natural and ordinary meaning of "collect" would, therefore, probably include some instances in which material has not been directly requested or invited, but would not include instances in which material is received accidentally, due to a misunderstanding, or without any indication having been given of an interest in receiving the material. For example, if a postage stamp collector is given postage stamps as gifts, and she puts them in her stamp album, she has collected them. Even though she has not directly asked for them, she has made her general interest in stamps known, she has a purpose for keeping them, and she has added them systematically to her existing collection. If, on the other hand, someone misunderstands her interest and gives her a rubber stamp, she would not have collected this stamp even if, through sheer inertia, she never gets around to throwing it away. Even without the express exclusion of unsolicited information, then, the Privacy Commissioner, the Tribunal or the courts may interpret "collect" as excluding some cases of receipt of unsolicited information.[261] The question is whether the exclusion of all unsolicited information from the meaning of "collect" is appropriate.

---

258 Telecom New Zealand, submission on Discussion Paper 1 for Privacy Commissioner Review of the Privacy Act 1993, 23 October 1997.

259 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.5, 151,805.

260 Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (South Melbourne, Oxford University Press, 2005) 214.

261 See *OA v New South Wales Department of Housing* [2005] NSWADT 233, para 36: "The mere receipt of a communication from the member of the public does not constitute a 'collection' of personal information, as it does not involve an act on the part of the agency of 'assembling' or 'gathering' the information (see definitions of 'collect' and 'collection' in *Macquarie Dictionary*, (1st ed, 1980)." The NSW Administrative Decisions Tribunal considered that the express exclusion of unsolicited information in section 4(5) of the Privacy and Personal Information Protection Act 1998 (NSW) simply put the matter beyond doubt.

3.95 To "solicit" is to "ask repeatedly or earnestly for or seek or invite" or to "make a request or petition to (a person)". "Unsolicited" means "not asked for; given or done voluntarily".[262] "Solicit" clearly has a narrower meaning than "collect", and would seem to require either a direct request to an individual or some kind of invitation (whether that be to specific people or to the public at large). As noted above, the Privacy Act 1988 (Cth) currently defines "solicit" in terms of requesting someone to provide information. Guidance from the Federal Privacy Commissioner in Australia states that an agency asks for or solicits information if it encourages people or organisations to give it information, including asking directly for information, arranging for information to be provided to it regularly, or encouraging people to give it information by such means as setting up a hotline.[263]

3.96 If the term "unsolicited" is considered in isolation, then, there is some sense to the argument that the unsolicited information exception means that certain types of surveillance are excluded from the coverage of the collection principles. Where a CCTV camera sits passively recording images of people it is hard to see how the information obtained can be said to have been solicited from the people who have been recorded by the camera. They are not asked if they want to be filmed, and they may not even be aware that they are being recorded. The unsolicited nature of such surveillance is even more obvious if the camera is hidden. However, if the meaning of "unsolicited" is considered in context as part of the definition of "collect", matters are less clear. As noted above, "collect" suggests making some effort to acquire information or acquiring it purposefully or systematically. It is probably only information that the agency has made no attempt to acquire that the unsolicited information exception is intended to exclude. The Office of the Privacy Commissioner website states that:[264]

> To collect information, the agency must, in some way, ask to get it. This includes setting up equipment to record anything that happens in an area. It is not a "collection" if the agency is just given information that it did not ask for.

The overall purpose of and background to the Act, including the desire to protect people against collection by unlawful, unfair or unreasonably intrusive means (principle 4), suggest that surveillance should be considered a form of collection of information. This is supported by the Explanatory Memorandum to the OECD Privacy Guidelines, which states that the Collection Limitation principle is directed, in part, at such practices as "the use of hidden data registration devices such as tape recorders".[265] Certainly, if it were not for the unsolicited information exception, there could be little doubt that a CCTV camera is collecting information in the ordinary meaning of the word "collect".

262 Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (South Melbourne, Oxford University Press, 2005) 1073, 1237. See also the definition of "unsolicited" in the Unsolicited Goods and Services Act 1975, s 2(1): "**Unsolicited** means, in relation to goods sent to any person, that they are sent without any prior request made by him or on his behalf."

263 Office of the Privacy Commissioner (Australia) *Plain English Guidelines to Information Privacy Principles 1–3* (Sydney, 1994) 4.

264 "Glossary" at www.privacy.org.nz/glossary (accessed 17 September 2009).

265 Explanatory Memorandum to the OECD Privacy Guidelines, para 52.

3.97 Information received by complaints bodies as part of a complaint should also probably fall within the definition of "collect" already. Such information is solicited in the sense that it is asked for or invited in a general way by the agency, even if the agency has not specifically requested each individual complaint. Internally-generated information is more ambiguous. Even without the exclusion of unsolicited information, it could be debatable whether a record of the fact that a particular transaction took place or that a particular disciplinary decision was taken constitutes a collection of that fact. In terms of the current definition of "collect", it is also hard to see how such information can be said to have been "solicited".

3.98 It appears, therefore, that there is at least some room for uncertainty about the meaning of "collect", and some matters that could be put beyond doubt by amending the definition in some way. There are three options for reforming the definition of "collect": deleting it, amending it, or clarifying it by means of guidance from the Privacy Commissioner.

3.99 The first option would be to remove the express exclusion of receipt of unsolicited information; in other words, to leave "collect" undefined. This would mean abolishing the distinction between solicited and unsolicited information, and should be considered together with our proposal in chapter 4 to adopt the ALRC's recommendation with regard to the treatment of unsolicited information. This approach would clearly deal with Paul Roth's point about collection and surveillance. It would, however, leave some continuing uncertainty about the scope of the term "collect". It is also possible that simply deleting the current definition would be interpreted as an indication that Parliament intends that all forms of unsolicited information should be considered to be collected for the purposes of the Act. We do not think that information which an agency has taken no steps to obtain should be considered to have been collected by that agency, although we do propose in chapter 4 that, if the agency does not destroy the information, it should treat it in the same way as if it had been collected.

3.100 The second option would be to revise the definition of "collect". This, in turn, could be done either by retaining the existing definition but adding a definition of "solicit" or "unsolicited", or by changing the definition so that it is not based on excluding unsolicited information but instead tries to spell out more clearly what "collect" means. The definition of "collect" in the report to the Minister of Justice on the Privacy of Information Bill, quoted above, is an example of the latter approach. The main problem with this approach is that it could be difficult to come up with a satisfactory definition. One possibility would be to leave the current definition of "collect", but add to it some specific provisions making clear that certain types of information (such as surveillance information and transaction records) are included in the definition. Another approach would be to define more precisely what is *excluded* from the definition: for example, the definition could exclude information obtained by mistake or sent to the agency without any form of request for the information having been made by the agency.

3.101 A third option, which could be combined with one of the first two options, would be for the Privacy Commissioner to develop guidance on these matters. The ALRC has recommended that the Office of the Privacy Commissioner should develop guidance about the meaning of "unsolicited" in the context of the collection principle in the Privacy Act 1988 (Cth).[266]

3.102 We propose that the definition of "collect" should simply be deleted, thereby removing the exclusion of receipt of unsolicited information. This would be consistent with the approach in most other jurisdictions and with the ALRC's proposed approach in Australia, and would remove problems with the current definition, particularly in relation to surveillance. It would be supported by the proposal in chapter 4 that agencies that receive unsolicited information should either destroy it or, if they retain it, treat it in the same way as if it had been actively collected. Other changes to the collection principles proposed in chapter 4 should also be considered in relation to the discussion of the definition of "collect".

Q20 We propose that the definition of "collect" should be deleted. Do you agree? If not, should it be clarified in some way?

OTHER TERMS

3.103 Other chapters discuss the definitions of particular terms relevant to those chapters. For example, the definitions of "agency", "news activity" and "news medium" are discussed in chapter 5. However, there may be other terms used in the Act that are currently undefined but that should be defined; or terms that are currently defined but whose definitions should be amended. For example, the terms "hold" and "obtain" could be defined, or the term "publicly available publication" could be amended to clarify its application to online information.

Q21 Are there any other terms that need to be defined, or whose definitions should be amended?

266 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 21-4, 726.

Chapter 4

The information privacy principles

4.1 The privacy principles are fundamental to the operation of the Privacy Act, so considering whether their effectiveness could be improved must be a key part of reforming the Act. This chapter identifies some issues for possible reforms to the existing principles, and also asks whether any new principles should be added to the Act.

BACKGROUND

4.2 The Privacy Act 1993, like information privacy legislation in other countries, sets out principles for regulating the handling of personal information. In New Zealand, these principles are known as information privacy principles. There are 12 of them, and they are found in section 6 of the Act. The current principles are set out in full as Appendix A to this issues paper.

4.3 The immediate origin of the privacy principles lies in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) of the Organisation for Economic Cooperation and Development (OECD). The OECD Guidelines include eight "basic principles of national application" which represent minimum standards for personal data protection in OECD member countries.[267] New Zealand's privacy principles are based on the OECD principles, but modify and expand on them in some respects. They were also influenced by the Information Privacy Principles in section 14 of the Australian Federal privacy legislation, the Privacy Act 1988 (Cth).[268]

4.4 Since the Privacy Act 1993 was passed, further sets of privacy principles have been articulated at the transnational level, or included in or proposed for national legislation. These include the principles in the Privacy Framework of the Asia-Pacific Economic Cooperation (APEC) group and the European Union's Data

267 The OECD Guidelines are discussed, and the eight principles set out in full, in New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, Wellington, 2008) 166–168. The principles in the OECD Guidelines are to be inserted as a schedule to the Privacy Act by the Privacy (Cross-Border Information) Amendment Bill 2008, no 221-2, cl 8B (inserting new Schedule 5A).

268 *Necessary and Desirable* 58.

Protection Directive,[269] as well as principles applying to the private sector in Canada and Australia.[270] The Australian Law Reform Commission (ALRC), in its Review of Australian Privacy Law, has given careful attention to the privacy principles, and has recommended a set of Unified Privacy Principles (UPPs) that would apply to both the public and private sectors.[271] The Australian Government has accepted that a single set of principles should apply to the public and private sectors, and has largely accepted the ALRC's recommended privacy principles, although with some amendments.[272] In considering whether any changes are needed to the privacy principles, we have taken account of features of these other sets of privacy principles that differ from those in the Privacy Act 1993.

REFORM OF THE PRINCIPLES

4.5 We have stated in chapter 2 our current view that the Privacy Act should continue to be based on an open-textured and flexible regulatory approach, rather than an approach based on "bright line" rules. It follows from our preference for an open-textured approach that the privacy principles should, as much as possible:

- be high-level statements of standards and responsibilities for agencies handling personal information;
- not be detailed or prescriptive, at least in their positive form (there is room for a higher level of detail in the exceptions);
- be general in scope and application (they should not apply only to particular types of information, particular sectors or particular technologies); and
- be "simple, clear and easy to understand and apply".[273]

4.6 These criteria should be borne in mind in considering how the existing principles might be revised, as well as whether any new principles should be added. Provisions that are very detailed or that apply only to particular types of agency, for example, should not be included in the principles but in another section of the Act.

269 The APEC Privacy Framework and the EU Data Protection Directive are discussed in New Zealand Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, Wellington, 2008) 169–170, 171–175. The EU Directive does not set out a discrete set of principles, but a number of the Directive's articles effectively constitute principles similar to those found in other privacy frameworks.

270 The Personal Information Protection and Electronic Documents Act SC 2000 c 5 is the Federal legislation governing privacy in the private sector in Canada. Schedule 5 of the Act incorporates ten privacy principles based on the Canadian Standards Association's *Model Code for the Protection of Personal Information*. The Privacy Act 1988 (Cth) was amended in 2000 (with the amendment coming into effect in 2001) to extend the Act's coverage to the private sector. A new set of National Privacy Principles applying to the private sector was included as Schedule 3 to the Act.

271 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) chs 18–32. The Model Unified Privacy Principles are set out in ibid, 91–102.

272 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 37–82.

273 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 653.

4.7 There are a range of options for the principles, from leaving them completely unchanged to starting again from scratch. In between these two ends of the spectrum are options such as:

- amending the existing principles in various respects;
- combining some of the existing principles;
- deleting some of the existing principles (either deleting them altogether or moving them to other sections of the Act);
- separating the principles from the exceptions; and
- adding new principles.

4.8 At this stage, the Commission does not support starting again from scratch with a completely new set of principles. We believe the existing principles have, by and large, worked well, and are broadly in line with internationally-accepted principles for the fair handling of personal information. While the ALRC has recommended a new set of privacy principles for Australia, the situation in Australia is different from that in New Zealand: the ALRC is seeking to harmonise two existing sets of national principles and several sets of principles operating at the state level. New Zealand already has a single set of principles that apply to the whole country, and to the public and private sectors.

4.9 The Commission can see no good reason why the existing principles should not be amended or added to, providing there are convincing arguments for each particular proposed amendment or addition. Adding new principles need not upset the sequence or numbering of the existing principles. Combining or deleting principles, however, would change the existing numbering and sequence, and could lead to some confusion until people became familiar with the new numbering. Any benefits from combining or deleting principles would therefore have to be weighed against the advantages of sticking with a set of principles that users of the Privacy Act are already familiar with. The interaction of any changes to the principles with the rules in codes of practice made under the Act (see chapter 7) would also need to be considered. The rules in Codes are based on the principles, but expand on or modify them in ways that are relevant to the particular context that the Code in question deals with.

Combining or deleting principles

Combining

4.10 Equivalent legislation in other countries combines some of the principles that are separated in New Zealand's Privacy Act. For example, the four collection principles can be combined in various ways, and the following pairs of principles could each be combined into a single principle: access and correction (6 and 7); security and retention (5 and 9); and use and disclosure (10 and 11). However, in our view wholesale combination of principles is not desirable for two reasons:

- it would upset the structure of the existing principles that people are familiar with; and
- having separate principles is more user-friendly and helps to draw people's attention to important topics.

4.11 The strongest case can be made for combining the use and disclosure principles. It is unusual internationally to have separate use and disclosure principles: the New South Wales Law Reform Commission (NSWLRC) calls it "a peculiarity of Australasian privacy legislation".[274] It would be relatively easy to combine them as their exceptions are almost the same – they differ only in that principle 11 has two extra exceptions. It could also help to clarify which principle applies when it is unclear whether a particular action is a use or a disclosure. Furthermore, combining principles 10 and 11 would leave the numbering of principles 1–9 unchanged.

Q22 Should any of the existing principles be combined?

Deleting

4.12 In our view, all of the existing principles serve a purpose and should remain in the Act. However, there is one possible candidate for removal from the principles themselves: principle 12 (unique identifiers). Principle 12 clearly stands out as being different from the other 11 principles, and in the Privacy of Information Bill as introduced it was not a principle, but was dealt with in another clause of the Bill. By all accounts it is the least used and least understood of the principles. It is not a cross-cutting principle that applies to personal information in general: it applies to a particular type of information. It also seems more prescriptive and less flexible than the other principles.

4.13 On the other hand, it probably does no real harm for the unique identifier provisions to be treated as a principle. If the provisions contained in principle 12 were to be removed to another part of the Act, thought would need to be given to where these provisions should be placed, and what other consequential changes would be needed. For example, section 66 would need to be amended so that an action in breach of the unique identifier provisions could constitute an interference with privacy for the purpose of the complaints provisions.

Q23 Should principle 12 be removed from the principles and placed somewhere else in the Act?

Q24 Should any other principles be deleted?

The exceptions

4.14 Principles 2, 3, 10 and 11 include exceptions in the body of the principles themselves, and we discuss these exceptions in this chapter. These exceptions constitute legitimate grounds for non-compliance with the principles. For example, all four principles allow non-compliance where this is "authorised by the individual concerned". There is a significant amount of overlap between the exceptions for these four principles. In particular, the exceptions for principles 2 and 3, and for principles 10 and 11, are very similar.

274 New South Wales Law Reform Commission *Privacy Principles* (NSWLRC R123, Sydney, 2009) 133.

4.15 The exceptions to principle 6 are not included in the body of the principle itself, but in Part 4 of the Act ("Good reasons for refusing access to personal information"). These exceptions are discussed in this chapter. Other exclusions and exemptions in the Act are discussed elsewhere in this issues paper, particularly in chapter 5. Exceptions relating to law enforcement are discussed in chapter 12. In addition, the provisions of other laws can effectively create exceptions to the privacy principles, as discussed in chapter 11.

4.16 It would be possible to separate the exceptions from the principles by moving them to another section of the Act and simply stating all of the principles in positive terms. This is the approach taken in the Data Protection Act 1998 (UK).[275] Some rewording of the existing principles would be needed in order to accomplish this. One advantage of taking the exceptions out of the principles would be that the principles would be simpler and less cluttered by detailed exceptions. This might make them easier to understand. There is also a lot of repetition in the exceptions to principles 2, 3, 10 and 11, although they are not identical so it may not be possible to come up with a set of generic exceptions that would apply to all four principles. Against these points, it can be argued that the exceptions are integral to principles 2, 3, 10 and 11, so it would be misleading and unhelpful to separate them out. Furthermore, users of the Act are familiar with their current location, and moving the exceptions may simply cause confusion while bringing only limited benefits. We favour retaining the exceptions to principles 2, 3, 10 and 11 as part of the principles, rather than placing them in another section of the Act.

4.17 Another possible change would be to move the exceptions to principle 6 into the body of the principle itself. This is the approach taken in the access and correction principles in the National Privacy Principles in the Privacy Act 1988 (Cth), and in the ALRC's Model Unified Privacy Principles. However, we do not think it would be desirable to make this change due to the length of the exceptions to principle 6.

4.18 Submitters are also welcome to suggest new exceptions to any of the principles.

Q25 Should there be any structural changes to the exceptions to the principles?

275 Data Protection Act 1998 (UK), schs 1 to 4.

COLLECTION PRINCIPLES

4.19 Principles 1 to 4 deal with the purposes for which information is collected, the collection of information directly from the person if possible, notification of certain matters to the individual concerned before or near the time of collection, and the means by which information may be collected. The definition of "collect" is discussed in chapter 3.

Principle 1 – purpose of collection

Defining purpose

4.20 The concept of "purpose" of collection is central to the privacy principles. Principle 3(1)(b) provides that, where an agency collects information directly from the individual concerned, it is to take reasonable steps to ensure that the individual is aware of the purpose of collection. Principles 10 and 11 provide that personal information is only to be used or disclosed for the purposes for which it was obtained, or for a directly related purpose. As discussed in chapter 3, "obtaining" appears to include both collecting information and receiving unsolicited information. The word "purpose" also appears in principles 7, 8 and 9, in relation to the accuracy and retention of personal information. Those principles do not refer to the purposes for which the information was collected, however, but rather the "purposes for which the information may lawfully be used" (principles 7 and 9) or the "purpose for which the information is proposed to be used" (principle 8).

4.21 It is inherent in principle 1 that an agency must have identified the purpose or purposes for which it is collecting personal information. There may, however, be a problem about how these purposes can be made known, or how to be certain about what the purpose of collection was if an issue arises at some later time. Principle 3(1)(b) requires agencies to notify the individual concerned of the purpose of collection, but if the information is not collected directly from the person, no such requirement applies.

4.22 There does not seem to be any easy answer to the question of how purposes can be specified more clearly and transparently. Agencies could be required to publish statements of the purposes for which they collect and hold personal information, although such statements might be so general as to be of little value. A requirement to specify publicly the purposes for which information is collected could be part of a new "Openness" principle, as discussed at the end of this chapter. The benefits of achieving greater clarity about purposes would have to be weighed against the compliance costs of any requirement to publish statements of the purposes of collection, particularly for agencies that are individuals or small businesses.

4.23 Section 87 of the Act provides that, in the case of proceedings relating to complaints under the Act, the onus of proving any exception provided for in the privacy principles is on the defendant. Thus, if an agency seeks to rely on the argument that its use or disclosure of personal information was not in breach of the principles because it was done for a purpose for which the information was obtained or a directly related purpose, the agency would be required to prove its purpose for obtaining the information.

4.24 There is no mechanism in the Act by which an agency can change the purposes for which it holds information, if it wants to be able to use or disclose information for purposes other than those for which it was collected, apart from going back to the individuals to whom the information relates to seek their authorisation for such a change of purpose. We understand from our consultations that some agencies might want to be able to change the purposes for which they hold information after it has been collected. It would appear to be inconsistent with the approach of the Act if agencies could do so unilaterally, without authorisation from the individuals concerned, and we do not believe they should be allowed to do so.

Q26 Are you aware of situations in which the purposes for which agencies collect information are unclear? Does a lack of clarity about the purpose for which agencies collect information sometimes cause problems? Do you have any suggestions about how the Act should deal with specification of purpose?

Reasonableness

4.25 At present principle 1 has no requirement of reasonableness in relation to the purpose of collection. Such a requirement could be expressed in terms of two questions:

- Are the purposes for which the information is being collected reasonable, having regard to the agency's functions or activities?
- Is the collection reasonably necessary to achieve those purposes?

There are examples of such requirements in some Canadian information privacy statutes.[276]

4.26 It does not seem practical or helpful to require that the purpose of collection be reasonable, since one person's reasonable purpose is another's unreasonable purpose. However, whether collection is reasonably necessary for the purpose does seem capable of more objective assessment. Paul Roth has observed that the "necessity" test (collection of information must be necessary for the agency's purpose) has not been applied very strictly in the Privacy Commissioner's case notes relating to complaints of breaches of principle 1. In a number of case notes cited by Roth, it appears that, in forming an opinion about the necessity of collection, the Commissioner may have assessed necessity solely or primarily from the standpoint of the agency against which the complaint was made.[277] If this is indeed a problem, one solution may be to amend principle 1 to provide that collection must be "reasonably necessary" for the purpose.

4.27 "Reasonableness", however, can be a double-edged sword, and depending on how it is interpreted it could either strengthen or weaken the "necessity" test. In the only Tribunal case to have considered the application of the necessity test, *Lehmann v CanWest Radioworks Ltd*, the Tribunal noted that:[278]

276 See for example Personal Information Protection Act SA 2003 c P-6.5 (Alberta), s 11.

277 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) para PVA 6.4(c).

278 *Lehmann v CanWest Radioworks Ltd* [2006] NZHRRT 35, para 47.

> The use of the word "necessary" in Principle 1(b) is not qualified. Taken at face value, the word might convey a sense of that which is essential; something but for which the purpose cannot possibly be achieved. If interpreted in that way, Principle 1 imposes a very high standard indeed for agencies to have to achieve before it can be said that the collection of personal information is justified within Principle 1.

The Tribunal concluded that principle 1 was intended to set a standard that is workable and achievable in the particular circumstances and "should be approached as setting a standard of reasonable rather than absolute necessity".[279] In this case, the Tribunal saw a reasonableness standard as making it more practical and achievable for agencies to comply with the necessity test in principle 1.

4.28 By contrast, a number of submitters to the ALRC review supported a reasonableness test in which what is reasonable is assessed from the perspective of a reasonable person, and not that of the agency collecting the information.[280] The ALRC agreed with this point of view, but did not think it was necessary to provide expressly in the Act for an objective test of reasonableness.[281] The NSWLRC, however, has recommended that the Collection principle should state that collection must be *reasonably* necessary, and further that there should be an objective test of reasonableness as follows: "the standard to be applied in determining whether the matter is reasonable or unreasonable … is what a reasonable person would consider appropriate in the circumstances".[282]

Q27 Should principle 1 be amended to require that the collection of information is *reasonably* necessary for the purpose? If so, how should reasonableness be determined?

Principles 2 and 3 – collection from and notification to the individual concerned

Collection "directly" from the subject

4.29 Paul Roth has suggested that collection of information by means of intermediary devices such as cameras or audio recording devices may not constitute collection "directly" from the person concerned, and may therefore not be covered by principle 3. In response, the Privacy Commissioner has recommended that the word "directly" be deleted from principle 3.[283] This seems to be a worthwhile change to remove any ambiguity. Moreover, the word "directly" does not seem to serve any useful purpose in either principle 2 or principle 3, and we propose that it be deleted from both. An alternative would be to provide specifically that principle 3 applies to collection of information by means of recording devices.

279 *Lehmann v CanWest Radioworks Ltd* [2006] NZHRRT 35, para 50.

280 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 729.

281 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 730–731.

282 New South Wales Law Reform Commission *Privacy Principles* (NSWLRC R123, Sydney, 2009) 35–37. The NSWLRC recommendation is modelled on provisions of the Personal Information Protection Act of the Canadian province of Alberta.

283 *3rd Supplement to Necessary and Desirable*, 2–3, rec 19A.

Q28 We propose that the word "directly" should be deleted from principles 2(1) and 3(1). Do you agree?

Unsolicited information

4.30 We have discussed the meaning of "collect" in chapter 3, and proposed that the current definition in the Act should be deleted. This would mean that "collect" would no longer exclude receipt of unsolicited information. Regardless of whether or not the definition of "collect" is deleted, however, there is a question about how unsolicited material should be treated. It could be desirable to spell this out more clearly. Where an agency decides to retain unsolicited material, it clearly "holds" that material for the purpose of later principles. But how does the concept of the purpose in connection with which the information was "obtained" (see the use and disclosure principles) apply? The ALRC has recommended that, where an agency receives unsolicited information, it must either:[284]

(a) if it is lawful and reasonable to do so, destroy the information as soon as practicable, without using or disclosing it except for the purpose of deciding whether it should be retained; or

(b) comply with all the relevant provisions of the privacy principles that apply to the information in question, as if the agency had taken active steps to collect the information.

The Australian Government has accepted this recommendation.[285]

4.31 We propose that a clause to this effect should be added to principle 2. The clause should also provide that an agency cannot retain information that it would not have been lawful for it to have collected.

Q29 We propose that principle 2 should provide that unsolicited information must either be destroyed; or, if it is retained, handled in compliance with all relevant provisions of the privacy principles as if the agency had take active steps to collect it. Do you agree? We further propose that principle 2 should provide that an agency must not retain unsolicited information that it would be unlawful for it to collect. Do you agree? Do you have any other suggestions with regard to the handling of unsolicited information?

Notification where information is not collected from the person concerned

4.32 The requirement in principle 3 that the individual concerned should be made aware of various matters relating to the collection of personal information applies only where the information is collected (directly) from the individual. In this respect, the New Zealand Act is narrower than some overseas legislation. For example, the National Privacy Principles in the Privacy Act 1988 (Cth) require

284 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 726, rec 21-3.

285 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 41.

notice to be given regardless of whether the information is obtained from the individual or from someone else. The ALRC recommends that this should continue to be the case in the UPPs.[286]

4.33 Principle 3 could be amended to require notification of the person concerned where information is collected from someone else. There will be good reasons why this should not happen in particular cases, but such reasons should be covered adequately by:

- the provision in principle 3 that agencies are required to take only "such steps (if any) as are, in the circumstances, reasonable" to notify the person; and
- the exceptions in principle 3.

If this change were to be made, however, the existing exceptions to principle 3 might need to be reconsidered.

Q30 Should principle 3 be amended by making it applicable whether or not the information is collected from the person concerned?

Exceptions

Prejudice to the individual's interests

4.34 Principles 2 and 3 provide for an exception where the agency believes on reasonable grounds that non-compliance "would not prejudice the interests of the individual concerned".[287] We believe this exception has the potential to unreasonably limit the protection of privacy. The agency collecting the information may not be in a good position to determine whether or not there will be any prejudice to the individual's interests. In a complaint involving a photograph taken of a man in a shopping mall and used in promotional material without his authorisation, the shopping mall sought to rely on this exception. The Privacy Commissioner commented that:[288]

> the mall was not in a position to determine what would prejudice the interests of shoppers…. [W]hat may be considered prejudicial will often depend on the individual concerned. For example, an individual in a witness protection scheme may consider that having their picture taken at a shopping mall would endanger them. Further, the collection and use of such photographs may be culturally offensive to some individuals.

Moreover, the focus on the interests of the individual could excuse agencies from complying in ways that, cumulatively, have negative consequences that go wider than the interests of particular individuals. We propose that this exception be deleted.

286 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 782 and rec 23-2.

287 Principles 2(2)(c) and 3(4)(b).

288 *Shopper Complains About His Photograph being Taken for Publicity Purposes* [2006] NZPrivCmr 1 – Case Note 60017.

4.35 Rules 2 and 3 of the Health Information Privacy Code 1994 (HIPC) do not include this exception, but instead allow for non-compliance where compliance would "prejudice the interests of the individual concerned".[289] While this formulation is preferable to a "no prejudice" exception, we do not think it is necessary to include it in principles 2 and 3 of the Act itself. Situations in which compliance would prejudice the interests of the individual concerned (such as emergencies in which a delay to seek to collect information from the individual might prejudice the individual's safety) should be able to be dealt with under the "not reasonably practicable" exception or the new "health or safety" exception proposed below.

"Not reasonably practicable"

4.36 Another existing exception to principles 2 and 3 provides that it is not necessary for agencies to comply with the requirements of these principles if an agency believes on reasonable grounds that compliance "is not reasonably practicable in the circumstances of the particular case".[290] We consider that this is a necessary and sensible exception, but we wonder whether there may be some ambiguity about what "reasonably practicable" means. It will clearly not be reasonably practicable to collect information from an individual, or to provide an individual with the information required by principle 3, if, for example:

- it is impossible, or unreasonably difficult, to contact the individual;
- the individual is incapable of providing or receiving information (for example, the individual might have a significant mental disability such that he or she cannot understand what is being asked or provide accurate answers); or
- the information that is being collected is the opinion of a third party (such as a doctor) about the individual.

It is worth noting that some instances in which compliance may be considered not to be reasonably practicable may also be covered by a separate exception which relates to situations in which "compliance would prejudice the purposes of the collection".[291]

4.37 While we support the retention of the "not reasonably practicable" exception for situations like those listed above, we do not think the exception properly applies to cases in which the agency wishes to avoid complying with principle 2 simply because the individual concerned refuses to provide the information, or because the agency believes that the individual would refuse.[292] We seek views on whether the Act should expressly provide that the "reasonably practicable" exception does not apply to such situations. We stress that, if the Act were to so provide, other exceptions might still apply to allow collection other than from the individual concerned.

289 Health Information Privacy Code 1994, rr 2(2)(c)(i), 3(4)(b)(i).

290 Principles 2(2)(f) and 3(4)(e).

291 Principles 2(2)(e) and 3(4)(d).

292 Although not concerned with principle 2, the Tribunal case of *Clearwater v Accident Compensation Corporation* [2004] NZHHRT 2, paras 103, 114, provides some support for our view: see discussion in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA6.5(g).

Health or safety

4.38 Principles 2 and 3 do not have an equivalent exception to the "health or safety" exception in principles 10 and 11. Rule 2 of the HIPC does, however, include an exception for situations in which the collection of information directly from the individual would "prejudice the safety of any individual".[293] There is such an exception in the ALRC's proposed Collection principle, although it applies only where the individual is incapable of giving consent:[294]

> the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent.

We propose that a health or safety exception should be included in principle 2, and perhaps principle 3.

Two exceptions to principle 3

4.39 The Privacy Commissioner in *Necessary and Desirable* recommended two changes to the exceptions to principle 3:[295]

- delete subclause (4)(a); and
- delete subclause (4)(f)(ii).

We propose that these deletions should be made.

4.40 Principle 3(4)(a) allows an agency not to comply with the notification requirements of principle 3 where non-compliance is authorised by the person concerned. The Privacy Commissioner noted that:

- This provision could be seen as allowing organisations to seek such authorisations on standard forms, in situations where there is an imbalance in the bargaining position between the individual and the agency.
- Authorisation needs to be informed, which is unlikely to be the case if the information required by principle 3 is not provided.
- Notification is a key provision of the Act, underlying other principles, particularly in terms of specification of purpose at the time information is collected.
- Such an exception is not generally found in privacy legislation overseas.

4.41 Principle 3(4)(f)(ii) allows for non-compliance with the notification requirements where the information collected "will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual". The Commissioner argued that, while a research exception was appropriate for principles 2, 10 and 11, it was not justified in principle 3 because:

- Where information is collected directly from the individual, there is nothing inherent in collection for research or statistical purposes that should excuse agencies from providing information to the person concerned about the purposes of collection and other matters.

---

293 Health Information Privacy Code 1994, r 2(2)(c)(iii).

294 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 733, UPP 2.5(c).

295 *Necessary and Desirable* 67–70, recs 20 and 21.

- The exceptions for situations where notification is not practicable or would prejudice the purposes of collection would still apply.
- A notification requirement appears to be in line with the code of practice of the Association of Market Research Organisations.

Q31 We propose that the "no prejudice" exception to principles 2 and 3 should be deleted. Do you agree?

Q32 Should the Act provide that the "not reasonably practicable" exception does not apply when an agency wishes to avoid complying with principle 2 simply because the individual concerned refuses to provide the information, or because the agency believes that the individual would refuse?

Q33 We propose that a "health or safety" exception should be added to principle 2. Do you agree? Should such an exception also be added to principle 3?

Q34 We propose that the exceptions in principle 3(4)(a) and 3(4)(f)(ii) should be deleted. Do you agree?

Principle 4 – manner of collection

4.42 Principle 4 seems to be one of the least problematic principles. It focuses on the "means" by which information is collected, and provides that such means must not be unlawful, unfair or unreasonably intrusive upon the personal affairs of the individual concerned. There could be a question about how principle 4 applies to collections in which there is nothing inherently intrusive or unfair about the means used to collect information, but the information that is sought is highly intrusive into an individual's personal affairs. For example, there is nothing inherently intrusive about a survey, but if the questions in a survey ask about very private matters it could be seen as being unreasonably intrusive. In our view, principle 4 is flexible enough to cover such situations. For example, we believe that if a survey were to ask questions that were, in the particular context, unreasonably intrusive, and if an individual felt under compulsion to answer the questions, this would be in breach of principle 4.

4.43 One area of uncertainty seems to be whether, or how, principle 4 applies to attempts to collect personal information, where no personal information is actually collected. The Human Rights Review Tribunal has discussed this issue in two cases, without deciding the matter.[296] In *Stevenson v Hastings District Council*, the Tribunal stated that:[297]

296 *Stevenson v Hastings District Council* [2006] NZHRRT 7, paras 64–72; *Lehmann v CanWest Radioworks Limited* [2006] NZHRRT 35, paras 67–68.

297 *Stevenson v Hastings District Council* [2006] NZHRRT 7, para 70.

> we do not wish to completely exclude the possibility that Principle 4 might apply to an unsuccessful attempt to collect personal information. We give a hypothetical example to illustrate our concern. What if an agency were to deliberately take unlawful steps in an effort to obtain personal information, but fail to achieve its objective only because of some event or circumstances beyond its control? Evidence establishes that the subject has suffered significant loss of dignity, humiliation and/or injury to feelings upon learning of the agency's conduct. In a case of that kind, we think it would be proper to consider whether the opening words of Principle 4 might have been intended to mean something like *"An agency shall not set about collecting personal information …"*. It seems to us to be at least arguable that such an approach reflects the legislative intention… .

4.44 In part, this issue reflects the fact that the Privacy Act is primarily about personal information, and may not be suited to dealing with invasions of privacy that do not involve the collection of information. Nevertheless, we believe that extending principle 4 so that it clearly covers attempts to collect information may provide people with a useful remedy in some cases where, for example, a person has been placed under unfair or unlawful surveillance but no personal information has been obtained as a result. We consider that it could help to clarify the Privacy Act's coverage of surveillance. As we have discussed in Stage 3 of our Review, the Privacy Act has an important part to play in ensuring that New Zealand law more comprehensively controls surveillance.[298]

Q35 We propose that principle 4 should be amended so that it clearly applies to attempts to collect information. Do you agree?

SECURITY, ACCURACY AND RETENTION PRINCIPLES

4.45 Principles 5, 8 and 9 are only loosely connected, but all could be seen as involving the fair and safe handling of personal information held by an agency: principle 5 says it should be kept secure, principle 8 says it should be checked for relevance and accuracy before it is used, and principle 9 says it should be kept no longer than necessary.

Principle 5 – security

4.46 The main gap in principle 5 concerns the issue of "browsing" (also referred to as "snooping" or "peeping") by employees of an agency who are authorised to access certain personal information but do so for purposes not connected with their employment.[299] Principle 5(a)(ii) states that agencies are to ensure that security safeguards are in place to protect against "access, use, modification, or disclosure, *except with the authority of the agency* that holds the information" (emphasis added). The words in italics would seem to exclude a situation in which a person is authorised by an agency to access information, but does so for an improper purpose. It is arguable that this situation would be covered by the reference to "other misuse" in 5(a)(iii), but this is not clear.

298 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC R113, Wellington, 2010) ch 4.

299 The term "peeping" comes from Peter Swire, and his article on the subject discusses this issue in greater depth: Peter P Swire "Peeping" Berkeley Tech LJ (forthcoming), available at www.ssrn.com.

4.47 The previous Privacy Commissioner discussed this issue in *Necessary and Desirable*. However, he focused on whether browsing, in the sense of simply looking at personal information without doing anything further with it, constitutes "use" of information for the purposes of the Act. He therefore recommended that consideration be given to enacting a definition of "use" which would include the retrieval, consultation or use of information; and that principle 5 should be amended by inserting the word "browsing" or "inspection" in principle 5(a)(ii).[300] There may be some value in this recommendation, but it does not seem deal with the major issue, which is that a person may be authorised to access information but may do so for an improper purpose.

4.48 Principle 5 could be amended to add "unauthorised consultation of personal information" to the list of prohibited activities, but this could still leave some ambiguity about the meaning of "unauthorised". If a person is authorised to access particular information, but does so for a purpose other than that for which he or she was given access, is such access unauthorised? Can this point be clarified in the Act? For example, a definition of "unauthorised access" could be added to the Act; or principle 5(a)(ii) could be amended by adding words such as "and in connection with the purposes for which the information is held by the agency" to the end of the subclause.

4.49 It appears that there is a significant gap in the law, especially when combined with section 252 of the Crimes Act which provides that the offence of accessing a computer without authorisation "does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access". We believe the gap needs to be filled by amending principle 5. We propose that principle 5 should be amended to make clear that agencies must take reasonable steps to ensure that people who are authorised to access personal information for the purposes in connection with which the information is held by the agency do not access, use, modify or disclose that information for other purposes.

Q36 We propose that principle 5 should be amended to make clear that agencies must take reasonable steps to ensure that people who are authorised to access personal information for the purposes in connection with which the information is held by the agency do not access, use, modify or disclose that information for other purposes. Do you agree?

Principle 8 – accuracy

4.50 Principle 8 differs from other data quality principles overseas in that it focuses on checking the accuracy of personal information *before use*. For example, the National Privacy Principle 3 in the Privacy Act 1988 (Cth) and the ALRC's UPP 7 say that an agency must take reasonable steps to ensure that personal information it "collects, uses or discloses" is accurate, complete and up-to-date. It should be noted, however, that New Zealand's Privacy Act also provides in principle 7(2) that an agency shall "if so requested by the individual concerned *or on its own initiative*" take reasonable steps to correct personal information that it holds to ensure that

300 *Necessary and Desirable* 53–55, 73–74, recs 16 and 23.

it is accurate, up-to-date, complete, and not misleading (emphasis added). This suggests that agencies have some ongoing responsibility to correct information that they hold if they have reason to believe that it may be inaccurate.

4.51 The main question for reform of principle 8 is whether "use" includes "disclose" for the purpose of principle 8 and, if so, whether this should be made clearer. While "use" in principle 8 should probably be interpreted as including disclosure, it is arguable that, given that the Act includes a separate disclosure principle, "use" in principle 8 has the same meaning as in principle 10. To avoid any lack of clarity, we propose that principle 8 should be amended to read "shall not use or disclose", as recommended by the Privacy Commissioner.[301]

Q37 We propose that principle 8 should be amended so that agencies must check the accuracy of information before use *or disclosure*. Do you agree?

Principle 9 – retention

Interaction with other laws

4.52 The issue of the interaction between principle 9 and the Public Records Act 2005 is discussed in chapter 11.

The question of purpose

4.53 A notable feature of principle 9 is that personal information is not to be retained "for longer than is required for the purposes for which the information may lawfully be used", rather than for the purpose for which it was collected. This is consistent with Australian legislation and with the ALRC's proposed principles, but differs from some overseas principles. For example, the principles in the Canadian private sector privacy legislation state that information shall be retained only so long as is necessary for the fulfilment of the purposes for which it was collected.[302]

4.54 One way of interpreting principle 9 is to read the words "may lawfully be used" as including the restrictions on use in principle 10. This would mean that information cannot be retained if it is to be used for a purpose other than that for which it was obtained, unless one of the exceptions in principle 10 applies. This does not seem to be the way in which principle 9 has been interpreted by the Privacy Commissioner, however. In case notes on two complaints involving principle 9, the Commissioner has contracted the phrase "purposes for which the information may lawfully be used" to "lawful purpose", which is arguably a somewhat different concept. The Commissioner has formed the opinion that an agency may retain information if it has a lawful purpose for doing so, without taking into account principle 10.[303] We do not suggest that this is an incorrect interpretation, simply that there may be some ambiguity in the meaning of principle 9.

301 *Necessary and Desirable* 79–80, rec 26.

302 Personal Information Protection and Electronic Documents Act SC 2000 c 5, sch 1, principle 5.

303 *Employee Discovers Employer Retained Suspension Details After Removal from File* [1998] NZPrivCmr 10 – Case Note 13066; *Man Objects to Retention of Information on Police Database* [2009] NZPrivCmr 5 – Case Note 204195.

4.55 Because the phrase "the purposes for which the information may lawfully be used" can be interpreted very broadly, it has been suggested to us that principle 9 is meaningless and should be deleted. According to this view, there will always be some purpose for which information can lawfully be used, and therefore retained, particularly historical or archival purposes. However, we have also heard a strong counter-argument, which is that principle 9 serves a useful purpose in focusing people's minds on the question of how long they need to retain personal information for. While principle 9 may not be very useful as an enforceable right, it is useful as a guide to good practice. Moreover, codes of practice can specify more precisely the periods for which information should be retained, as is the case in the Credit Reporting Privacy Code.[304]

4.56 One option, short of simply deleting principle 9, would be to amend it to expressly provide that information shall not be retained for longer than is necessary for the purpose for which it was *obtained*. However, this may be too narrow and impractical. There may good reasons why information should be retained even when it is no longer needed for the original purpose. In particular, it might be desirable to retain it for historical or other research purposes.

4.57 We find the arguments for the retention of principle 9 persuasive, and we do not currently see a need to amend it. It serves a useful purpose in drawing agencies' attention to the issue of retention, and can always be given greater specificity by a code of practice.

Q38 We propose that principle 9 should continue to allow retention of information for so long as it is required for the purposes for which it may lawfully be used. Do you agree?

Methods of disposal

4.58 Principle 9 currently discusses the duration of retention of personal information, but says nothing about what should happen to that information when a decision is taken to dispose of it. Some overseas principles refer to what should happen to information that is no longer needed. For example, the ALRC's proposed UPP8 (based on the existing National Privacy Principle 4 in the Privacy Act 1988 (Cth)) says that agencies should "destroy or render non-identifiable personal information if it is no longer needed". A discussion paper prepared for the *Necessary and Desirable* review makes the point that other options for information that is no longer needed include returning documents to the individual concerned or disclosing the information in accordance with principle 11 to another agency that does have a further lawful use for the information.[305] Because there are potentially many different ways in which information that is no longer needed could be acceptably disposed of, this issue is probably better dealt with by way of guidance from the Office of the Privacy Commissioner than by any amendment to the legislation.

304 These competing views of principle 9 were put to us at a meeting of people with particular expertise in relation to the Privacy Act, held at the Law Commission on 8 May 2008.

305 Office of the Privacy Commissioner *Review of the Privacy Act 1993: Discussion Paper No 2: Information Privacy Principles* (Wellington, 1997) 12.

Q39 We propose that principle 9 should continue not to specify how personal information should be disposed of. Do you agree? Would guidance on this point from the Office of the Privacy Commissioner be helpful?

ACCESS AND CORRECTION PRINCIPLES

4.59 Principle 6 provides individuals with a right to know whether an agency holds personal information about them and to have access to that information. Principle 7 provides that individuals are entitled to request the correction of information about them held by an agency or, if the agency refuses to make such a correction, to have attached to the information a statement of the correction sought but not made. The exceptions to principle 6 (grounds on which access to personal information can be refused) are contained in Part 4 of the Act. Part 5 of the Act contains procedural provisions relating to access and correction. Parts 4 and 5 of the Act are discussed here, as well as the provisions in the bodies of the principles themselves. Section 55 of the Act provides that principles 6 and 7 do not apply in respect of certain types of information. We have not identified any issues relating to section 55, but we ask a question about this section in chapter 5.

Principle 6 – access

4.60 There seem to be no problems with the wording of principle 6 itself. However, concerns have been raised about the issue of "coerced access requests".[306] This is where a third party such as an employer or an insurance company requires someone to use the right of personal access under principle 6 to obtain documents such as criminal or medical records. That is, the person obtains his or her own records but does so at the request of the third party, and the information is passed on to that third party. This would seem to be inconsistent with the intent of principle 6, and it is said to have been a growing problem since the Privacy Act was introduced. In part, the problem is that provisions in the Wanganui Computer Centre Act which prohibited coerced access to criminal records were repealed by the Privacy Act and not replaced. However, the issue is not restricted to criminal records, and coerced access to medical records by insurance companies has been a growing concern.[307]

4.61 Sections 56 and 57 of the Data Protection Act 1998 (UK) deal with this problem by prohibiting employers, prospective employers and service providers from requiring individuals to produce certain types of records (mainly criminal records) obtained by exercising their access rights; and voiding any term or condition of a contract that purports to require an individual to produce health records obtained by exercising their access rights. *Necessary and Desirable* essentially recommended the addition of similar provisions in the Privacy Act here.[308]

306 See discussion in *Necessary and Desirable* 363–367 and *4th Supplement to Necessary and Desirable* 31; Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA6.9(f).

307 Although it does not deal directly with the issue of coerced access under principle 6, see Privacy Commissioner "Collection of Medical Notes by Insurers: Inquiry by the Privacy Commissioner" (June 2009), available at www.privacy.org.nz.

308 *Necessary and Desirable* 363–367, recs 151 and 152.

4.62 At this stage the Law Commission has no views on the seriousness of this problem, whether the Privacy Act should be amended to deal with it, or what form any such amendment might take. We would welcome further information and submissions on this topic.

> Q40 Are coerced access requests a problem? If so, can the Privacy Act be amended to deal with the problem?

Principle 7 – correction

4.63 *Necessary and Desirable* recommended a straightforward amendment to principle 7, which we support. This amendment would require agencies to inform requesters, in cases where the agency is not willing to correct their personal information, of their right to request that a statement be attached to the information of the correction sought but not made.[309]

> Q41 We propose that where an agency is not willing to correct personal information, it should be required to inform the requester of his or her right to request that a statement be attached to the information of the correction sought but not made. Do you agree?

Good reasons for refusing access – Part 4 of the Act

4.64 The reasons for refusing access in the Privacy Act are based on those in the Official Information Act 1982 (OIA), so revision of the grounds in the Privacy Act might need to happen in tandem with revision of those in the OIA. The Law Commission also has on its work programme a review of the OIA, so the grounds in the OIA can be considered as part of that review. Grounds for refusal that relate to law enforcement are discussed in chapter 12.

4.65 The Privacy Commissioner has made recommendations for reorganisation of the reasons for refusing access to make them easier to follow.[310] These recommendations should be considered in the drafting of any Bill that may result from our final report on the Privacy Act.

Safety

4.66 At present section 27(1)(d) provides that access to personal information can be refused if its disclosure "would be likely to endanger the safety of any individual". The Complaints Review Tribunal held in *O v N* that this provision relates only to physical safety, not to health or "mental safety" (so, as discussed further below, it does not apply to harassment).[311] It is worth considering whether this should be expanded on.

309 *Necessary and Desirable* 76, rec 24.

310 *Necessary and Desirable* 147–148, rec 47; *2nd supplement to Necessary and Desirable* 9, 16–18.

311 *O v N* (12 March 1996) Complaints Review Tribunal 4/96, 15.

4.67 One option would be to bring it more into line with the health and safety exception in principles 10 and 11; that is, something like:

> would be likely to present a serious threat to:
>
> (a) public health or public safety; or
>
> (b) the life or health of any individual.

This would introduce:

- a seriousness element;
- a health element; and
- a public element.

It would also be broadly consistent with the Access and Correction principle in the Australian National Privacy Principles, and the ALRC's proposed Access and Correction principle. The latter refers to situations where "providing access would be reasonably likely to pose a serious threat to the life or health of any individual".

4.68 Another option would be to adopt a modified version of the wording of the OIA, section 9(2)(c): "Avoid prejudice to … the health or safety of members of the public" (the words "measures promoting" have been omitted).

4.69 Note that health reasons for refusing access also come up in section 29(1)(c), but these concern only the withholding of information where the individual's medical practitioner considers that disclosure of the information would be likely to prejudice the physical or mental health of the individual to whom the information relates.

Q42 Should the "safety" ground in section 27(1)(d) be expanded? If so, what new elements should it contain?

Harassment

4.70 An issue that is related to the safety ground is whether there should be a ground for refusal where there is a significant likelihood of harassment of an individual as a result of the disclosure. Such harassment might fall short of being a serious threat to safety, but could have a serious negative effect on a person's quality of life, as recognised by the enactment of the Harassment Act 1997. The previous Privacy Commissioner in *Necessary and Desirable* recommended that consideration be given to adding such a withholding ground.[312] He noted, however, that if such a change were to be considered it would be necessary to consider it for both the Privacy Act and the OIA, and that the issue is probably more pressing in relation to the OIA. In the case of the Privacy Act, information that could be used for the purposes of harassment could most likely be withheld on other grounds, such as maintenance of the law or avoiding disclosure of the affairs of another individual (sections 27(1)(c), 29(1(a)). There have been cases where information has been withheld under section 29(1)(a) (unwarranted disclosure of the affairs of another individual) because of concerns about

312 *Necessary and Desirable* 152–153, rec 49.

harassment.[313] Nevertheless, a specific withholding ground where there is a reasonable fear of harassment is worth considering, particularly in conjunction with an equivalent change in the OIA.

Q43 Should there be a specific withholding ground relating to significant likelihood of harassment, or do existing withholding grounds cover this adequately?

Commercial prejudice

4.71 The Privacy Commissioner has recommended that consideration be given to an amendment to section 28(1)(b) to allow an agency to refuse access to information where the disclosure would prejudice the commercial position of the agency itself, particularly in relation to the agency's bargaining position with the individual requesting the information.[314] At present refusal is allowed only where the disclosure would prejudice the commercial position of the person who provided or is the subject of the disclosure. The Privacy Commissioner noted that the commercial sensitivity withholding ground under the OIA has been controversial, and that any change to this ground in the Privacy Act would need to be considered together with the equivalent ground in the OIA.

Q44 Should the "commercial prejudice" withholding ground in section 28(1)(b) be amended? If so, how?

Mixed information about the requester and others

4.72 Section 29(1)(a) allows for the refusal of access to information where disclosure "would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual". This raises the question of how to deal with information that is a mixture of information about the requester and information about others; in other words, situations where the privacy interests of two or more people need to be balanced against each other. In *Necessary and Desirable* the then Privacy Commissioner said that such cases "involve some of the most difficult complaints that come before me". He also noted, however, that principles for dealing with such cases had been developing in the jurisprudence of the Ombudsmen, the Privacy Commissioner and the Human Rights Review Tribunal. He recommended that consideration be given to providing statutory guidance on the withholding of personal information in cases of "mixed" information.[315]

313 See *Patient Requests Names of Nurses who Attended her in Hospital* [2007] NZPrivCmr 7 — Case Note 93953; *M v Ministry of Health* (29 April 1997) Complaints Review Tribunal 12/97, in which the Tribunal held that the defendant agency had correctly distinguished between information that should be withheld under section 27(1)(d) on safety grounds and information that should be withheld under section 29(1)(a) because it might lead to individuals being subject to unwelcome contact from the requester.

314 *Necessary and Desirable* 155–156, rec 51.

315 *Necessary and Desirable* 157–158, rec 52.

4.73 While it could be difficult to draft statutory guidance on this issue, there is a possible model in the Data Protection Act 1998 (UK). Section 7(4) of that Act provides that, where an agency cannot comply with an access request without disclosing information relating to another identifiable individual, it is not obliged to comply with the request unless the other person has consented to the disclosure, or it is reasonable in the circumstances to comply with the request without the other person's consent. Section 7(6) clarifies the circumstances in which it might be reasonable to provide access without the other person's consent. Sections 7(5) and 8(7) provide further clarification about when information is considered to relate to another person, and when that person is considered to be identifiable from that information. Section 7(5) also provides that the agency is not excused from supplying as much of the information sought by the requester as can be provided without disclosing the identity of the other person.

4.74 Our provisional view is that any statutory guidance on this issue would be difficult to draft, and runs the risk of being convoluted (as the provisions in the UK Act arguably are). A better alternative could be for the Privacy Commissioner to provide guidance on the issue.

Q45 Should the Privacy Act be amended to provide statutory guidance with respect to the withholding of information under section 29(1)(a) in cases of "mixed" information? If not, would guidance from the Privacy Commissioner be of assistance?

Physical or mental health

4.75 The Privacy Commissioner recommended that consideration be given to amending the ground for refusal in section 29(1)(c) so that the agency could consult with the individual's psychologist as well as his or her doctor about withholding of information on health grounds. One legal practitioner with expertise in the privacy field has told us that she has encountered difficulties with section 29(1)(c) because it refers only to doctors and not other relevant health practitioners. Note that section 29(4) defines "medical practitioner" consistently with the Health Practitioners Competence Assurance Act 2003. This covers psychiatrists, but not psychologists, other mental health practitioners, or other health practitioners in general.

Q46 Should section 29(1)(c) be amended to refer to consulting the individual's psychologist when appropriate? Should it refer to consulting with any other health practitioners and, if so, which ones?

Repeated requests

4.76 The problem of repeated requests for the same information can take two forms:

- Requests for information that the individual has previously been unsuccessful in obtaining. Such requests could be vexatious in nature, but could also be motivated by a genuine desire to obtain access to information that the requester has been denied access to.
- Requests for information that has already been provided to the person. Such requests are more likely to be purely vexatious in nature, although in some cases there could be a genuine desire to obtain material that has been added to the file since the last request.

4.77 Agencies could already seek to rely on the "frivolous and vexatious" ground in section 29(1)(j). However, they may feel that they are on firmer ground if there is a specific provision dealing with this issue. The requests may not be frivolous in terms of their content, and it could be difficult to establish the requester's vexatious intent.

4.78 The Privacy Commissioner has suggested three possible ways of dealing with this problem. The first, based in part on a Law Commission recommendation for an amendment to the OIA,[316] is to add new grounds for refusing access to section 29 where:[317]

- a person making a request has already been refused access to the information requested, provided that no reasonable grounds exist for that person to request the information again; or
- a person making a request has already been given access to the information requested on a recent occasion, provided that no reasonable grounds exist for the person to request the information again.

4.79 An overseas provision that deals with the problem of repeat requests for information that has already been provided is the Data Protection Act 1998 (UK), sections 8(3)–8(4):

> (3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.
>
> (4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

316 New Zealand Law Commission *Review of the Official Information Act 1982* (NZLC R40, Wellington, 1997) 45.

317 *1st supplement to Necessary and Desirable* 5–6, rec 58A.

4.80 The Privacy Commissioner's second suggestion to deal with this problem is based on provisions in some Canadian privacy legislation. The Commissioner suggested that either the Commissioner or the Tribunal could be empowered to exempt an agency from having to deal with a particular individual's access request for a fixed period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operations of the agency and amount to an abuse of the right of access.[318]

4.81 The third suggestion, which is related to the second, is that the Commissioner should be able to enable a public sector agency to make reasonable charges for repeat requests. This would involve an amendment to section 36, and could act as a deterrent to such requests (private sector agencies are already entitled to charge for information requests).[319] It would also allow agencies to recover some of the costs of responding to repeat requests.

4.82 We currently favour the first of these options, and the formulation of the new ground for refusal proposed by the Privacy Commissioner. However, we would like to hear views on any of the options, or any additional options.

> Q47 We propose that a new ground for refusal should be added to allow agencies to refuse access to information that has previously been provided to an individual, or that has previously been refused, provided that no reasonable grounds exist for the individual to request the information again. Do you agree? Do you have any other suggestions about how the Privacy Act should deal with the problem of repeated access requests for the same information?

Access and correction – procedural provisions – Part 5 of the Act

Charging for correction

4.83 At present section 35(3)(b)(i) allows private sector agencies to charge for correcting personal information that they hold. It has been suggested that it is absurd to charge for correcting information when it is in the agency's interest to have correct information on file. The Privacy Commissioner recommended that section 35(3)(b)(i) should be deleted.[320] Our current view is that private sector agencies should not be allowed to charge for correction, but we would like to hear from the private sector in particular about the implications of such a change.

> Q48 We propose that private sector agencies should no longer be allowed to charge for correction of personal information. Do you agree?

318 *Necessary and Desirable* 187–188, rec 66.

319 *Necessary and Desirable* 188; *1st supplement to Necessary and Desirable* 6.

320 *Necessary and Desirable* 184–185, rec 65.

Responding to requests

4.84 The Privacy Commissioner has recommended adding a new ground for agencies to seek an extension of time for responding to an access or correction request.[321] The Commissioner recommended that complexity of the issues raised by the request should be added to the grounds in section 41(1). This is based on a Law Commission recommendation with regard to the OIA, which has not yet been implemented.[322] Our provisional view is that the Privacy Commissioner's recommendation should be supported.

> Q49 We propose that complexity of the issues raised by a personal information request should be added to the grounds for seeking an extension of time in section 41(1). Do you agree?

USE AND DISCLOSURE PRINCIPLES

4.85 As noted above, principles 10 and 11 differ from each other only in that principle 11 adds two more exceptions. In their positive form, they can be stated very simply: personal information should not be used or disclosed for purposes other than those for which the information was obtained. Consequently, most of the issues relate to the exceptions to these principles. As we have already noted, these principles refer to the purposes for which information was "obtained", rather than "collected". This appears to allow unsolicited information to be included in the coverage of principles 10 and 11.

Disclosure within agencies

4.86 There is some uncertainty about how principle 11 applies when personal information is disclosed within an agency (for example, from one co-worker to another). A decision by the Complaints Review Tribunal held that principle 11 did not apply to disclosures within an agency, on the grounds that section 3(1) of the Act provides that information held by a person in his or her capacity as an employee or officer of an agency is deemed to be held by the agency.[323] Both Paul Roth and the Privacy Commissioner disagree with this interpretation.[324] They argue that, if principle 11 is not intended to cover disclosures within agencies, this should be expressly stated. In more recent cases involving disclosures within agencies, the Human Rights Review Tribunal has managed to avoid ruling on this question.[325]

4.87 It would seem desirable to put this question beyond doubt, if a suitable form of words can be found. However, it is likely to be difficult to draft a provision that will adequately cover the issue. Our current view is that any statutory clarification

321 *Necessary and Desirable* 195–196, rec 71.

322 New Zealand Law Commission *Review of the Official Information Act 1982* (NZLC R40, Wellington, 1997) 67–68. See Official Information Act 1982, s 15A(1).

323 *KEH and PH v Department of Work and Income* (19 December 2000) Complaints Review Tribunal 40/2000.

324 *Church Elders Disclose Pastor's Marriage Difficulties to Congregation* [2002] NZPrivCmr 8 – Case Note 18541; Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA6.14(c)(xi).

325 *Ram v Kmart New Zealand* [2003] NZHRRT 27; *Clearwater v Accident Compensation Corporation* [2004] NZHRRT 2.

should provide that disclosures within agencies can fall within the coverage of principle 11. However, the difficulty will be in distinguishing between appropriate and inappropriate intra-agency disclosures.

Q50 Should the Act expressly provide that disclosures within agencies can be covered by principle 11? If so, how should this be done?

Disclosure of information that is already known

4.88 Paul Roth has discussed the question of disclosure of information that is already known by the person to whom it is disclosed.[326] He notes that the Privacy Commissioner and the Tribunal have taken the view that this does not constitute disclosure, providing that no additional new information is conveyed and that the audience is not a mixed one of people who know the information and people who do not know it. Roth considers it artificial to treat such situations as not involving disclosure, and suggests that there should instead be a new exception for such cases.

4.89 In a submission to the ALRC, the Cyberspace Law and Policy Centre argued that there should be protection against disclosure even where the information is known to the recipient:[327]

> Information received from an earlier non-authoritative source means less than the "same" information confirmed by a later more authoritative source. Organisations could abuse this simply by asking whether other organisations could "confirm" some item of information they purported to know, and the "confirmations" would not be disclosures. Where a recipient of information really does learn nothing from information received, any compensation resulting from that breach by disclosure is likely to be reduced, as the disclosure has had no effect on the data subject. On balance, therefore, it is better for "disclosure" to include previously known information.

This is a valid point, and suggests that Roth may be right to argue that the issue should not be dealt with by excluding information that is already known from the definition of disclosure. An exception does, however, seem to be needed to avoid absurd situations in which agencies feel that they cannot discuss information about a person that another agency clearly already knows. While the "harm" threshold could be used to weed out such cases that became the subject of complaints, this would not assist agencies when deciding whether or not to disclose. Furthermore, we propose in chapter 8 the removal of the harm threshold.

4.90 The issue raised by the Cyberspace Law and Policy Centre of agencies obtaining information by seeking to "confirm" information they purport to already know is perhaps something of a red herring in this context. If there were to be a new exception for disclosure of information that is already known by the recipient, there would still be protections in the privacy principles. Imagine that Agency

326 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA6.14(c)(i).

327 Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales "Implementing Privacy Principles: After 20 Years Its [sic] Time to Enforce the *Privacy Act*: Submission to the Australian Law Reform Commission on the Review of Privacy Issues Paper" (31 January 2007) 28.

A asks Agency B to "confirm" information that it purports to know about person X. Agency B would need to believe, on reasonable grounds, that Agency A does in fact already know this information about person X. Furthermore, Agency A is clearly breaching principle 4 by collecting information by unfair means.

4.91 At present we have no view on this issue. We would welcome submissions on whether this issue actually causes problems and, if so, how it should be dealt with.

Q51 Should there be a new exception to principle 11 where the disclosure is to a person or persons who already know the information in question?

Health and safety exception

4.92 The existing exceptions 10(d) and 11(f) cover situations where the use or disclosure for purposes other than those for which the information was obtained is allowed if that use or disclosure is necessary:

> to prevent or lessen a serious and imminent threat to –
>
> (a) public health or public safety; or
>
> (b) the life or health of the individual concerned or another individual.

4.93 The key question in relation to this exception is whether the threshold of "serious and imminent" is appropriate. It has been suggested to us that the threat should not have to be both serious *and* imminent. There will be cases where a threat is serious, but not imminent. For example, in cases involving disclosure of genetic information to an individual's relatives, the threat of a genetic condition that those relatives may carry could be very serious, but the condition might not show up for many years.

4.94 The ALRC has recommended doing away with the requirement that threats be imminent, and simply requiring that they be serious.[328] It argues that requiring threats to be both serious and imminent sets the bar too high. Further, the ALRC argues that the concept of "serious" necessarily involves an assessment of the likelihood of a particular outcome as well as how grave the consequences of that outcome might be. An event that is highly unlikely would not usually be described as a serious threat. Removing the imminence requirement would make assessment of *when* the threat might eventuate unnecessary, but an assessment of *whether* the threat was likely to occur would still be necessary. The ALRC emphasised that the exception would still contain important safeguards: the agency would still need to believe on reasonable grounds that the use or disclosure was *necessary* to lessen or prevent the threat, not merely desirable or convenient. Accordingly, the ALRC recommended that use or disclosure should be permitted if an agency reasonably believes that the use or disclosure "is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety".

328 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 859–861. This recommendation has been endorsed by the NSWLRC: New South Wales Law Reform Commission *Privacy Principles* (NSWLRC R123, Sydney, 2009) 137.

4.95 In a submission to the ALRC, the Cyberspace Law and Policy Centre supported the removal of the "imminent" element with regard to threats to individuals' health and safety, but opposed it in the case of threats to public health or safety. They argued that, in the absence of a requirement that the threat to public health or safety be imminent as well as serious, agencies could abuse this provision to claim exceptions "for bulk or routinised uses or disclosures… [I]t is difficult to see how claims could not be made under it for a wide range of law enforcement and welfare programmes, including high volume data-matching and data linkage projects".[329] There is something to this argument, but we are also persuaded by the ALRC's argument that "serious" already implies some assessment of whether something is likely to happen, and that it is only the question of *when* a particular threat is likely to eventuate that would be taken out of the equation. This, together with the reasonableness and necessity thresholds, would seem to address the concern raised by the Cyberspace Law and Policy Centre.

4.96 The Australian Government has accepted the ALRC's recommendation on this point, but with two amendments. First, the Australian Government's position is that agencies should be able to use the health and safety exception to use or disclose personal information only after the individual's consent has first been sought, where this is reasonable and practicable. Secondly, while the Australian Government agrees that the "imminence" test can be too restrictive, it also accepts the concerns of some stakeholders that removing the "imminence" test would excessively broaden the exception. It therefore proposes to pursue a compromise position.[330]

4.97 While we will await the wording of the Australian Government's compromise position with interest, we are not currently persuaded that there is any need to retain the "imminence" test. One option would be to change the exception to "serious *or* imminent". However, it is hard to see why there should be an exception for use and disclosure where a threat is merely imminent, but not serious. We propose that the "imminent" element should be deleted from the health and safety exceptions in principles 10 and 11.

Q52 We propose that the words "and imminent" should be deleted from principles 10(d) and 11(f). Do you agree?

329 Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales "Strengthening Uniform Privacy Principles: An Analysis of the ALRC's Proposed Principles: Submission to the Australian Law Reform Commission on the Review of Australian Privacy Law Discussion Paper 72" (17 December 2007) 40.

330 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 54.

UNIQUE IDENTIFIER PRINCIPLE

4.98 Principle 12 provides protections with regard to the assigning by agencies of unique identifiers. It provides that agencies shall not assign unique identifiers unless it is necessary to do so to enable the efficient carrying out of the agency's functions; shall not reassign a unique identifier assigned to the individual by another agency; shall take reasonable steps to establish the identity of a person before assigning a unique identifier to him or her; and shall not require an individual to disclose any unique identifier assigned to him or her except for one of the purposes in connection with which that unique identifier was assigned, or a directly related purpose. Unique identifier is defined as follows:

> **unique identifier** means an identifier—
>
> (1) That is assigned to an individual by an agency for the purposes of the operations of the agency; and
>
> (2) That uniquely identifies that individual in relation to that agency;—
>
> but, for the avoidance of doubt, does not include an individual's name used to identify that individual.

4.99 As discussed above, it can be argued that principle 12 is not a true principle at all and that it could be removed from the principles into another section of the Act. However, whether or not it remains a principle, some amendments to the current unique identifier provisions are worth considering.

Definitional issues

4.100 Principle 12 refers to assigning of unique identifiers by agencies. In *Necessary and Desirable*, the previous Privacy Commissioner considered whether the term "assign" should be defined in the Act.[331] He referred to situations in which agencies could be uncertain about whether a unique identifier has been "assigned", such as where the agency simply records the number on its files but makes no further use of it. The Commissioner concluded that it was best to rely on the ordinary meaning of the term and to allow the meaning to be clarified over time in real cases. We would like to know whether agencies encounter difficulties with interpreting the meaning of "assign", and whether it would help to define the term in the statute.

4.101 A second definitional issue concerns the meaning of "identifier". While "unique identifier" is defined, "identifier" is not, except to the extent that "an individual's name used to identify that individual" is excluded from the meaning of "unique identifier". The ALRC has recommended that "identifier" should be defined as including:[332]

> a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:
>
> (a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or
>
> (b) is determined to be an identifier by the Privacy Commissioner.
>
> However, an individual's name or Australian Business Number … is not an "identifier".

331 *Necessary and Desirable* 89–90.

332 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1040.

Two features of this definition are worth considering:

- it expressly includes symbols and biometric information; and
- it allows the Privacy Commissioner to determine that something is an identifier.[333]

4.102 It could be worth clarifying in the Privacy Act that "identifiers" can include symbols, biometric information and other particulars that can be used to identify an individual, although there is no reason why any particular other than an individual's name should be considered to be excluded from the current definition of "unique identifier". The use of biometric information to identify people or to verify their identities, using technologies such as finger scanning or facial recognition, raises privacy issues which are discussed further in chapter 13. The ALRC considered that the policy considerations underlying the Identifiers principle were also relevant to the use of biometric identifiers. However, the Australian Government believes that the collection of biometric information for identification or verification purposes "will not result in the privacy risks that the 'identifiers' principle is intended to address, such as the risk of an identifier becoming widely held and applied to facilitate extensive data-matching or data-linking." As a result, the Australian Government did not accept the ALRC's recommendation that the Identifiers principle should apply to biometric information.[334]

4.103 The ALRC's recommendation that the Privacy Commissioner should be able to determine that something is an identifier was apparently intended mainly to allow the Commissioner to determine that something can be an identifier for the purposes of the Identifier principle even though it does not *uniquely* identify an individual. The example was given, in the Australian context, of a Medicare number which might be shared by two or more family members, so that the number does not in fact uniquely identify each individual. A secondary reason for giving a determination power to the Commissioner was to allow the Commissioner to deal with any ambiguities about whether particular personal information was an identifier. The ALRC did not think that the power would need to be used often, and it recommended that any such determination should be a legislative instrument for the purposes of the Legislative Instruments Act 2003 (Cth), and therefore disallowable by Parliament.[335] It could be argued, however, that it is not constitutionally proper for the Commissioner to make determinations with regard to the meaning of a key term in the Act that he or she administers.[336] It appears that the Australian Government takes this latter

333 See discussion in Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 1035–1039.

334 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 74.

335 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1035–1037.

336 See also our discussion in chapter 10 of the option of allowing the Privacy Commissioner to make binding rulings.

view, since it has decided that the Minister responsible for the Privacy Act, rather than the Privacy Commissioner, should have the power to determine what a government identifier is for the purposes of the Act.[337]

Q53 Should "assign" or "identifier" be defined in the Act, and if so, how should they be defined?

Restricting principle 12(2) to public sector unique identifiers

4.104 Principle 12(2) provides that an agency shall not assign to an individual a unique identifier that has been assigned to that individual by another agency (unless the two agencies are associated persons within the meaning of the Income Tax Act). The previous Privacy Commissioner recommended that this prohibition should apply only to the reassignment of unique identifiers generated, created or assigned by public sector agencies, but that section 46(4) should be amended to make it clear that a code of practice may apply the controls in principle 12(2) to any unique identifier (whether originally assigned by a public or a private sector agency).[338] The Commissioner noted that this change would help to reduce some of the complexity and compliance costs associated with unique identifiers without reducing privacy protection. He also noted that the applicability of principle 12(2) to unique identifiers originally assigned by the private sector had led to problems in the superannuation industry, leading to the creation of the Superannuation Scheme Unique Identifier Code 1995. The concerns that led to the creation of the unique identifier principle were essentially with the use of unique identifiers, such as tax file numbers, created by government agencies. If problems were to arise in future with identifiers created by the private sector, this could be addressed by modifying principle 12(2) in a code of practice.

4.105 It is noteworthy that the ALRC recommends that controls on the assignment of unique identifiers in its proposed Identifiers principle should apply only to "organisations" (that is, to the private sector) and only to identifiers assigned by "agencies" (that is, by the public sector).[339]

Q54 Should principle 12(2) be amended so that it applies only to unique identifiers originally generated, created or assigned by public sector agencies (with an accompanying amendment to section 46(4) to allow principle 12(2) to be reapplied to private sector-generated identifiers by a code of practice)?

337 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 74.

338 *Necessary and Desirable* 90–91, rec 28.

339 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1049–1050.

Exceptions to principle 12(2)

4.106 At present, principle 12 contains only minimal exceptions. The only exception in principle 12(2) is for the reassignment of a unique identifier by an agency that is an "associated person" of the agency that originally assigned the identifier. The Privacy Commissioner has suggested that the Law Commission, in reviewing principle 12, should consider the usefulness of including exceptions in principle 12(2), having regard to the Australian experience with its identifier principle.[340] The Commissioner noted that several codes of practice have had to be issued in order to provide exemptions from principle 12(2).

4.107 The ALRC's UPP 10.3 (based on the existing National Privacy Principle 7.1A) provides that the controls on reassignment, use or disclosure of identifiers do not apply to prescribed organisations, identifiers and circumstances, as set out in regulations made after the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned. UPP 10.2 also provides exceptions to controls on the use or disclosure of identifiers where the use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier; where certain exceptions to the Use or Disclosure principle apply; or where the use or disclosure of an identifier that is genetic information would be permitted by proposed Privacy (Health Information) Regulations.

4.108 A specific issue that has been raised with us concerns the lack of an exception to principle 12(2) for statistical and research purposes. The question is whether any general exceptions, such as for statistical and research purposes, should be included in principle 12(2). If it is considered desirable to add exceptions to principle 12(2), the wording of some the exceptions in the other principles could perhaps be used.

> Q55 Should there be an exception to principle 12(2) for statistical and research purposes? Should there be any other exceptions to principle 12(2)?

Requiring an individual to disclose a unique identifier

4.109 Principle 12(4) provides that an agency shall not require an individual to disclose a unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned, or for a directly related purpose. This raises the question of whether, or in what ways, it is possible to use documents containing unique identifiers (such as drivers' licenses and passports) as forms of identification. Paul Roth cites a 1995 conference paper by Blair Stewart of the Office of the Privacy Commissioner in which Stewart:[341]

340 *4th supplement to Necessary and Desirable* 9–11, rec 28A.

341 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA6.15(d), quoting Blair Stewart "Information Privacy Principle 12 and the Superannuation Schemes Unique Identifier Code 1995" (address to the IIR 5th Annual Super Fund and Funds Management conference, Auckland, 27 November 1995) 6.

comments that there are a number of unanswered legal issues arising from Principle 12(4). He queries whether the term "require" involves an element of compulsion (such as denial of a particular service if the demand for disclosure of the unique identifier is refused by the individual), or whether it includes "a simple invitation to establish eligibility by means of providing that number or by any other legitimate means". Another related issue is whether the demand for a particular document that contains the unique identifier can amount to a requirement to disclose the unique identifier itself. In this context, Blair Stewart remarks:

> … one of the concerns is that the agency ends up by holding the unique identifier. Accordingly, if an agency needs to see a copy of some evidence of identity for some legitimate reason it would seem desirable that they do not simply take a copy of the driver's licence which may be produced if it involves unnecessarily recording the unique identifier. The agency may need only to record the fact that a licence was produced. If they require some record identifying the documentation it may be that licence will have a document number which will satisfy all legitimate needs without the need to also note the individual's unique identifier as a licenced driver. It is also preferable that individuals be given a choice as to acceptable documentation to produce identity or eligibility.

Q56 Is there any uncertainty about the application of principle 12(4)? If so, how should this be addressed?

Enforceability of principle 12(2)

4.110 The Privacy Commissioner has commented that the existing complaints and enforcement procedures are unlikely to be effective in relation to principle 12(2), because any breaches are likely to be done on a system-wide, rather than an individual basis; and because it may be difficult to show any immediate harm to the individual, even though the reassignment of a unique identifier may lead to future harm in the form of information sharing in breach of principles 2, 10 or 11. The Commissioner recommended an amendment to section 66(1) so that a wilful breach of principle 12(2) would be an interference with privacy even in the absence of harm.[342]

4.111 In chapter 8 we propose removing the harm threshold for all complaints. However, if the harm threshold is not to be removed for all complaints, its removal should still be considered in relation to principle 12(2).

Q57 Are any other changes needed to any of the existing privacy principles (including the provisions relating to principles 6 and 7 in Parts 4 and 5 of the Act)?

342 *Necessary and Desirable* 91–92, rec 29.

POSSIBLE NEW PRINCIPLES

4.112 On the whole, we think the existing privacy principles have provided an adequate framework for the protection of informational privacy. Nonetheless, this review is an opportunity to consider whether any new principles should be added. There are some other principles that either exist already in overseas legislation, or have been proposed by law reform bodies or commentators. Of these principles, we think the strongest case exists for adding principles dealing with anonymity and pseudonymity, and openness. We therefore discuss these principles at greater length, before concluding the chapter with a brief discussion of other possible principles.

Anonymity and pseudonymity

4.113 Where an individual interacts anonymously with an agency, that individual cannot be identified in any way. In other words, the agency collects none of the individual's personal information, or perhaps only so much personal information as can be collected without the individual becoming identifiable. An individual interacts pseudonymously with an agency when the individual uses a pseudonym or alias that is not related to his or her usual name. Often the pseudonym will be specific to the particular interaction, although sometimes an individual may choose to use the same pseudonym in different contexts. Using a pseudonym allows a person to be traced through multiple transactions even though the agency has no way of knowing who the person behind the pseudonym is. In contexts in which reputation can be important (such as online trading), pseudonymity has the advantage of allowing for the accrual of "reputational capital" by the person's alias; that is, over time the alias can acquire a positive or negative reputation through its interactions with others.[343]

4.114 An Anonymity principle exists already in the National Privacy Principles in the Privacy Act 1988 (Cth) and also in the Information Privacy Act 2000 (Vic). The ALRC has recommended the following wording for its Anonymity and Pseudonymity principle:[344]

> Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:
>
> (1) not identifying themselves; or
>
> (2) identifying themselves with a pseudonym.

This recommendation has been accepted by the Australian Government.[345]

343 Ken D Kumayama "A Right to Pseudonymity" (2009) 51 Ariz L Rev 427, 444.

344 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 708 (UPP 1).

345 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 39.

4.115 In New Zealand, the Privacy Commissioner recommended that consideration be given to adding a second part to principle 1 stating that "wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering transactions". In a subsequent report, the Commissioner recommended that the wording of the ALRC's proposed Anonymity and Pseudonymity principle be adopted.[346]

4.116 Strictly speaking, an Anonymity principle could be viewed as unnecessary. An agency that collects information about a person's identity when it does not need to do so for the purpose for which it is collecting information would be breaching principle 1. However, in the absence of a specific provision to this effect, agencies may overlook this requirement. As the Privacy Commissioner has suggested, anonymity and pseudonymity could be covered in a new subclause of principle 1; or it could be a separate, stand-alone principle.

4.117 The ALRC makes the following comments in support of its recommendation for an Anonymity and Pseudonymity principle:[347]

> [A]n anonymity principle encourages agencies and organisations to consider the fundamental question of whether they need to collect personal information at all and to design their systems accordingly. Secondly, allowing individuals to retain greater control over their privacy by giving them the option to transact anonymously, where appropriate, will potentially give rise to significant public policy benefits. For example, this option might encourage an individual to seek medical or other assistance from an organisation or agency where, if the assistance was contingent on the individual identifying himself or herself, the individual would be discouraged from seeking the assistance. This can be illustrated by the anonymous supply of sterile syringes and needles to injecting drug users, which is an important public health initiative in all Australian states and territories. As well as face-to-face outlets, some needle and syringe programs include automatic dispensing machines, to accommodate people who wish to avoid interpersonal contact altogether.
>
> Agencies' concerns about the practical application of the principle can be accommodated adequately within the broader limitations of the principle—that is, that the option for anonymity must be provided only where it is "lawful and practicable". …
>
> The ALRC recommends that the anonymity principle should [also] provide for pseudonymous transactions. This provides a more flexible application of the principle, by covering the situation where it would be impracticable or unlawful for an individual to transact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with an agency or organisation. An extension of the principle to encompass pseudonymous transactions will also encourage agencies and organisations to incorporate into their systems privacy-enhancing technologies that facilitate pseudonymous interactions in an online environment.

346 *1st supplement to Necessary and Desirable* 23–24, rec 17A (incorrectly numbered 17B); *4th supplement to Necessary and Desirable* 5–6.

347 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 693, 696.

> Two principal objections to a pseudonymity requirement were raised in submissions: the cost of implementation, particularly where it would have a relatively limited application; and the potential to detract from the accuracy of records. These issues can be accommodated adequately within the broader limitations of the "Anonymity and Pseudonymity" principle—that is, transacting anonymously or pseudonymously must be "lawful and practicable".

4.118 In the United Kingdom, an independent report on the *Database State* has recommended that citizens should have the right to access most public services anonymously. The report argues that a right to anonymity can help to curb the increasing intrusiveness of government data collection, and minimise discrimination in service provision.[348] We think any such right should not be limited to interactions with the public sector, however.

4.119 We consider that the concepts of anonymity and pseudonymity have an important role to play in the protection of privacy. However, we are undecided about whether specific provisions about these matters should be added to the privacy principles, given that they can be seen as being already implicit in principle 1.

Q58 Should an anonymity and pseudonymity principle be added to the Privacy Act, either as part of principle 1 or as a separate principle? If so, what should be the content of such a principle?

Openness

4.120 In contrast to the notification requirements in principle 3, which apply when information is collected from individuals, an openness principle would require agencies to have information generally available (for example, in privacy policies available on their websites) about their collection and use of personal information. As we discuss in chapter 6, such a principle was originally included in the Privacy of Information Bill, in order to implement the Openness principle in the OECD Guidelines. The inclusion of the principle was widely criticised, however, so it was dropped, and instead section 21 of the Privacy Act provided for the compilation by the Privacy Commissioner of directories of personal information held by agencies. In chapter 6 we propose that section 21 should be deleted, but this leaves the question of whether the Act should provide in some other way for transparency about the information-handling practices of agencies.

4.121 The ALRC has recommended that there should be a separate Openness principle. It argues that such a requirement should be additional to, and separate from, the requirement to notify individuals of certain matters when information is collected from them (principle 3 of the New Zealand Privacy Act):[349]

> It is not appropriate to deal with requirements relating to openness and notification in the same principle because of their important conceptual differences. Openness provisions require agencies and organisations to make their general practices relating to

348 Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath and Angela Sasse *Database State: A Report Commissioned by the Joseph Rowntree Reform Trust Ltd* (Joseph Rowntree Reform Trust, York, 2009) 43–44.

349 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 809–810.

the handling of personal information transparent. The requirement is not targeted exclusively for the benefit of those whose personal information has been, or is to be, collected. The obligation attaches regardless of whether an agency or organisation has actually collected personal information from a particular individual, or plans to do so.

In contrast, the requirement to notify or otherwise ensure an individual is aware of specified matters under the "Notification" principle applies *only* when an individual's personal information has been, or is to be, collected. Further, the "Notification" principle is directed to informing the particular individual how the agency or organisation will, or is likely to, handle his or her personal information, or personal information *of the kind* collected from the individual.

The benefits that flow from compliance with the openness requirements therefore can be distinguished in their nature and scope from those relating to notification. The publication of explanations as to how agencies and organisations deal with personal information generally benefits the regulatory system as a whole. It allows, for example, the Office of the Privacy Commissioner (OPC) to monitor an agency's or organisation's compliance with the *Privacy Act* and also to recommend changes to the personal information management practices of the agency or organisation. Openness, therefore, plays a key role in promoting best practice in the handling of personal information.

The NSWLRC has also supported an Openness principle, considering that it would help to "promote a culture of trust and reliability between the public, whose personal information is collected, used, stored and shared, and the agency who must handle that information in order to perform its function."[350]

4.122 The ALRC's Openness principle would require agencies to create, and make available without charge, privacy policies setting out their policies on the management of personal information, including how personal information is collected, held, used and disclosed. Specifically, the ALRC recommended that privacy policies should outline:[351]

- the sort of personal information the agency holds;
- the purposes for which personal information is held;
- the avenues of complaint available to individuals if they have a privacy complaint;
- the steps individuals may take to gain access to personal information about them held by the agency; and
- whether personal information is likely to be transferred outside Australia, and the countries to which such information is likely to be transferred.

4.123 The Australian Government has accepted the ALRC's recommendation for an Openness principle. In addition to the matters specified in the ALRC's principle, the Australian Government has decided that the principle should require agencies to take reasonable steps, having regard to the agency's circumstances, "to develop and implement internal policies and practices that enable compliance with the Privacy Principles." Such policies and practices could include providing training

350 New South Wales Law Reform Commission *Privacy Principles* (NSWLRC R123, Sydney, 2009) 109.

351 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 829 (UPP 4.1).

to staff, establishing complaints procedures, developing information explaining the agency's policies and procedures, and establishing procedures to identify and manage privacy risks and compliance issues.[352]

4.124 We think that, for the reasons given by the ALRC and the NSWLRC and accepted by the Australian Government, there is much to recommend the creation of an Openness principle. However, we are also aware that it could be seen as imposing a compliance burden for small agencies. Most large agencies probably already have privacy policies which they make available on their websites, but it might be unrealistic to expect many small businesses to prepare privacy policies. It should also be borne in mind that an individual can be an agency for the purposes of the Privacy Act. Some threshold for complying with the Openness principle would need to be established, therefore, or at least the principle would need to provide that agencies are required to take only such steps as are reasonable, having regard to the nature and circumstances of the agency. Another possible criticism of the Openness principle is that the privacy policies developed by agencies would, in many cases, be so general as to be of little value. For example, a large agency might collect personal information for many different purposes, and it might be difficult to set all of these purposes out in a policy in any meaningful way. We are also aware that the inclusion of an Openness principle in the Privacy of Information Bill was subject to significant criticism. We are therefore interested to hear whether submitters see value in the creation of an Openness principle, or whether there are other ways in which transparency with regard to information-handling practices could be provided for.

Q59 Should the Privacy Act include an Openness principle? If so, what should be its content? If not, should openness be provided for in some other way?

Other possible principles

4.125 A number of other possible new principles are set out briefly below. Further discussion of these principles can be found in the report of the ALRC. We do not currently propose that any of these principles should be included in the Privacy Act. Submitters are also welcome to propose new principles that are not listed below.

4.126 **Accountability.**[353] This principle would require agencies to take some responsibility, with regard to personal information that they transfer to third parties, for ensuring that those third parties have in place adequate privacy protection. This would be one way of addressing the issue of transborder data flows, as discussed in chapter 14. Where personal information is transferred from one agency within New Zealand to another, the receiving agency is already obliged to comply with the Privacy Act, so an accountability principle seems unnecessary with regard to domestic transfers.

352 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 "For Your Information: Australian Privacy Law and Practice"* (Canberra, 2009) 48–50.

353 See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1132–1134.

4.127 **Consent.**[354] New Zealand's Privacy Act deals with consent as an exception to some of the principles. An alternative approach found in some overseas statutes is to require consent as the norm, and to make consent a principle, in which case there would need to be exceptions for situations in which consent was not needed.[355] We believe that the New Zealand approach of treating consent as an exception to the principles is the correct one, and that making it a separate principle would unduly elevate it relative to other considerations.

4.128 **Prevention of harm.**[356] This principle would require agencies to take steps to prevent harm to individuals by the misuse of personal information, and to provide remedial measures for any such harms that occur. We consider that this principle is so vague as to be meaningless, and is adequately covered by the principles taken as a whole. The related question of whether there should be an obligation to notify an unauthorised disclosure of data is discussed in chapter 16.

4.129 **No disadvantage.**[357] This principle would provide that agencies should not unfairly disadvantage a person for asserting his or her privacy rights. For example, an agency should not charge a fee or refuse to provide a service to a person who insists on receiving notification in accordance with principle 3. We are not aware of any such principle in the privacy laws of other jurisdictions. We believe that this issue is best dealt with through specific provisions, such as the existing restrictions on charging for access requests. Also relevant are provisions in some of the privacy principles that agencies must take such steps as are reasonable, since unfairly disadvantaging people would surely be seen as unreasonable.

4.130 **Sensitive information.**[358] Many overseas information privacy statutes, including the Privacy Act 1988 (Cth) and the Data Protection Act 1998 (UK), make special provision for a category of "sensitive" information such as information about a person's racial or ethnic origin, political and religious opinions and affiliations, sexual orientation and criminal record. Such provisions do not necessarily take the form of a separate principle, although there is such a principle in the National Privacy Principles in the Privacy Act 1988 (Cth). Perhaps more commonly, there are specific provisions in some privacy principles about how those principles apply to sensitive information. We do not believe there is any need for such a category of information in New Zealand, and consider that the designation of certain types of information as particularly sensitive is likely to be somewhat arbitrary. Some types of sensitive information, such as health information, can be dealt with by codes of practice. The sensitivity of particular information is also a matter that agencies should already consider in relation to principle 4, in assessing whether the collection of personal information is unreasonably intrusive into personal affairs.

---

354 See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) ch 19.

355 This is the approach taken in the Personal Information Protection and Electronic Documents Act SC 2000 c 5, sch 1, principle 3.

356 See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1134–1136.

357 See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1136–1139.

358 See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) ch 22.

4.131 **Transborder data flows and direct marketing.**[359] These issues are discussed in chapters 14 and 15. While there is certainly a case for specific provisions in the Privacy Act dealing with these issues, we are not convinced that adding new principles dealing with either issue is the best approach. Principles should ideally be high-level and applicable to personal information generally, rather than to particular types or uses of information.

4.132 **Data breach notification.** We discuss data breach notification in chapter 16. If mandatory data breach notification were to be introduced in New Zealand, one option would be to introduce it into the Privacy Act by means of a new principle or part of an existing principle, with more detailed provisions elsewhere in the Act. In chapter 16 we propose that, if data breach notification is to be made mandatory, the obligation to notify could be introduced by amending principle 5, rather than by means of a separate principle.

Q60 Should any other new principles be included in the Privacy Act? If so, what are they?

359 See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) chs 26 and 31, as well as chs 14 and 15 of this issues paper.

Chapter 5

Exclusions and exemptions

5.1 A number of provisions in the Privacy Act limit the application of the privacy principles in various ways, or exempt certain entities or types of information from the application of the privacy principles altogether. This chapter examines some key provisions in the Act that create exclusions and exemptions from the privacy principles. A number of other types of exclusions, exemptions and exceptions are discussed in other chapters of the issues paper.

BACKGROUND

5.2 Privacy is not an absolute right, and other rights or interests will sometimes take precedence over it. For example, privacy interests may be outweighed by such public interests as national security, health and safety, or freedom of information. By providing for exclusions, exemptions and exceptions, information privacy laws recognise the need to balance privacy against such other interests.

5.3 International human rights and privacy instruments recognise that the right to privacy can legitimately be limited for various reasons. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that no one shall be subjected to "arbitrary or unlawful" interference with privacy. This wording implies that interferences with privacy will sometimes be allowed, providing they are lawful and are not arbitrary. The Human Rights Committee, the body with official responsibility for monitoring implementation of the ICCPR, has recognised in a General Comment on article 17 that "As all persons live in society, the protection of privacy is necessarily relative." However, any interferences with the right to privacy must be authorised and specified by law, must comply with the aims and objectives of the ICCPR, and must be reasonable in the circumstances.[360] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data also contemplate that states may create

360 Human Rights Committee "General Comment 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17)" (8 April 1988). See also European Convention for the Protection of Human Rights and Fundamental Freedoms, art 8(2), which permits only such interference with the right to privacy 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."

exceptions to the principles set out in the Guidelines, but state that such exceptions should be as few as possible and should be made known to the public.[361]

5.4 Blair Stewart of the Office of the Privacy Commissioner notes that drafting and locating exceptions to privacy laws "is not a technical matter of little importance", since such exceptions define the extent of the privacy principles. Getting exceptions right, he continues, can enhance:[362]

- the workability of a law;
- the clear understanding of legal obligations;
- the appropriate workload of a small Privacy Commissioner's office;
- the timeliness of sorting out business compliance difficulties;
- the flexibility of the law; and
- the appropriate response to lobbying for special favours.

5.5 Distinctions can be drawn between the following ways in which the Act provides that the privacy principles may not apply, or that their application may be modified, in certain cases:[363]

- **Exclusions** refer to entities or types of information that are not covered by the privacy principles at all. For example, the privacy principles do not apply at all to the news media in the course of their news activities (with a limited exception for Radio New Zealand and Television New Zealand).
- **Exemptions** provide that particular types of agency or information, although not excluded altogether from the scheme of the Act, do not have to comply with certain privacy principles. For example, the intelligence organisations are required to comply only with principles 6, 7 and 12. Alternatively, the application of some privacy principles to certain agencies could be modified so that the principles are easier to comply with.
- **Exceptions** are general in application, and allow for particular privacy principles not to be complied with on certain grounds. That is, they place limits on the scope of the principles themselves. There are detailed exceptions in several of the principles. For example, there are exceptions to principles 2, 10 and 11 that allow for collection, use or disclosure of personal information that is publicly available.

5.6 In this chapter we discuss entities that are excluded from the coverage of the privacy principles by being excluded from the definition of "agency", and certain exemptions provided for in Part 6 of the Act. Other exclusions, exemptions and exceptions are discussed elsewhere in the issues paper:

- Some information is excluded from the coverage of the Act by the definitions of "individual" and "personal information", as discussed in chapter 3. In particular, the Act does not apply to information about deceased persons or legal persons.

361 Organisation for Economic Development and Cooperation "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980), para 4. See also paras 46–47 of the Explanatory Memorandum to the Guidelines.

362 Blair Stewart "The New Privacy Laws: Exemptions and Exceptions to Privacy" (paper presented to The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).

363 See Blair Stewart "The New Privacy Laws: Exemptions and Exceptions to Privacy" (paper presented to The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).

- Chapter 4 discusses exceptions contained in the principles themselves, as well as the "good reasons for refusing access" (which are effectively exceptions to principle 6) set out in Part 4 of the Act.
- Codes of practice, discussed in chapter 7, can modify the application of the principles by prescribing standards that are more or less stringent than those that would normally apply, or by exempting any action from any privacy principle. Codes that provide for less stringent standards are effectively a type of exemption.
- The Act provides for authorised information matching programmes in the public sector, as discussed in chapter 9. Such programmes are effectively exempted from the application of the privacy principles, and are instead subject to a set of information matching rules set out in Schedule 4 to the Act.
- As discussed in chapter 11, other laws can override the Privacy Act, effectively creating exceptions to the application of the privacy principles.
- Law enforcement exceptions are discussed in chapter 12.

EXCLUSIONS FROM THE DEFINITION OF "AGENCY"

5.7 Section 2(1) of the Privacy Act provides that an agency means "any person or body of persons, whether corporate or incorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a Department". However, the definition goes on to state that certain entities or types of entity are excluded from the definition of "agency". The definition of "agency" does not include:

(i) The Sovereign; or

(ii) The Governor-General or the Administrator of the Government; or

(iii) The House of Representatives; or

(iv) A member of Parliament in his or her official capacity; or

(v) The Parliamentary Service Commission; or

(vi) The Parliamentary Service, except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee; or

(vii) In relation to its judicial functions, a court; or

(viii) In relation to its judicial functions, a tribunal; or

(ix) An Ombudsman; or

(x) A Royal Commission; or

(xi) A commission of inquiry appointed by an Order in Council made under the Commissions of Inquiry Act 1908; or

(xii) A commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter; or

(xiii) In relation to its news activities, any news medium.

5.8 The effect of these exclusions is that the listed entities are not required to comply with the privacy principles, since the principles refer to information that is collected, held, used or disclosed by an agency, or in the case of principle 12, to unique identifiers that are assigned by an agency. Entities that are excluded from the definition of "agency" therefore cannot breach the privacy principles, which in turn means that they cannot be the subject of complaints about breaches of the principles. It is important to note, however, that there is nothing to prevent

the Privacy Commissioner from commenting or reporting on the actions of entities that are excluded from the definition of "agency", pursuant to her general functions relating to "the privacy of the individual" under section 13 of the Act.

5.9 At present, the entities excluded from the definition of "agency" are thereby exempted from all of the privacy principles, although in some cases the exemptions are limited in certain respects (for example, members of Parliament are only exempted in their official capacities). In considering options for reform, it should be borne in mind that these entities could be made subject to some but not all of the principles, if it is considered desirable that certain privacy principles should apply to them.

5.10 We are not aware of any issues that require consideration with regard to the exclusions of the Sovereign, Governor-General or Administrator, courts, tribunals, or Royal Commissions or other public inquiries. In relation to courts and tribunals, we note that their exclusion applies only to the exercise of their judicial functions. In our *Access to Court Records* report, we considered whether this exclusion extended to court records even after a matter is finally determined and all appeal rights have been exhausted. We concluded that it did, and that the Privacy Act does not apply to court records.[364] Privacy is, however, recognised in court rules as a matter to be taken into account when considering applications for access to court documents, files or records.[365] With regard to the various forms of public inquiry, the Law Commission's report on *A New Inquiries Act* recommended that privacy should be one of the grounds for restricting public access to inquiries, and this is reflected in the Inquiries Bill currently before Parliament.[366]

House of Representatives and Members of Parliament

5.11 The House of Representatives is excluded from the definition of "agency", and MPs are excluded in their "official capacity". The then Privacy Commissioner discussed these exceptions in *Necessary and Desirable.* With regard to the House of Representatives, the Commissioner noted that privacy is protected to some degree by Standing Orders and other rules and practices of the House. He concluded that if any of the privacy principles (particularly the access principle) were to be applied to the House, this should be done by Standing Orders rather than by statute, and that it would be best for the initiative to come from Parliament itself. He recommended that the matter be considered by an appropriate committee of Parliament.[367]

5.12 With regard to MPs, the Commissioner noted that the exclusion of "a member of Parliament in his or her official capacity" goes beyond the exemption that would apply as an incidence of Parliamentary privilege. For example, constituency work would fall within the category of activity carried out in the Member's official capacity. The Commissioner suggested that there would probably be few

364 New Zealand Law Commission *Access to Court Records* (NZLC R93, Wellington, 2006) 55–56.

365 Criminal Proceedings (Access to Court Documents) Rules 2009, r 16(c); Judicature Act 1908, sch 2 (High Court Rules), r 3.16(b); District Court Rules 2009, r 3.22(b).

366 New Zealand Law Commission *A New Inquiries Act* (NZLC R102, Wellington, 2008) 94–95; Inquiries Bill 2008, no 283-1, cl 15(2)(d).

367 *Necessary and Desirable* 36–37, rec 5.

problems in applying some principles, such as principles 4 and 5, to MPs, while others (such as the disclosure principle) would be much more controversial. He raised a particular concern about what happens to personal information in MPs' constituency files when a Member loses office. Again, the Commissioner recommended that the matter be considered by an appropriate committee of Parliament.[368]

5.13 Our provisional view is that these matters should be considered by a committee of Parliament, as recommended by the Privacy Commissioner.

> Q61 We propose that the application of the privacy principles (not necessarily by way of the Privacy Act itself) to the House of Representatives and to MPs should be considered by a committee of Parliament. Do you agree?

Parliamentary Service Commission and Parliamentary Service

5.14 The Parliamentary Service Commission is entirely excluded from the definition of "agency". The Parliamentary Service is excluded "except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee". The Office of the Clerk is covered by the Privacy Act.

5.15 In *Necessary and Desirable*, the Privacy Commissioner noted that the then General Manager of the Parliamentary Service could see no reason why the Parliamentary Service, in fulfilling its administrative functions, should not be fully subject to the Act, providing that this could be accomplished without impinging on the exemption for MPs in their official capacities. The Commissioner recommended that either the partial exemption of the Parliamentary Service should be further restricted or the Service should be made fully subject to the Privacy Act, so long as the General Manager's caveat could be accommodated. The Privacy Commissioner also recommended that the exemption for the Parliamentary Service Commission be reviewed to see whether it could be replaced with a partial exemption.[369]

5.16 The Commissioner subsequently considered these exemptions further in a report on the Parliamentary Service Bill, and his recommendations in that report were also included in a supplement to *Necessary and Desirable*. In his report on the Bill, the Commissioner commented that:[370]

> The two exceptions to the Privacy Act primarily reflect a desire to place certain information off limits to access requests. This approach largely continues the thinking which had previously led to complete exemption of the Official Information Act. One of the most important reasons for the exemptions is the fact that members of Parliament themselves have never been subject to the Official Information Act, and are exempted in their official capacities from the Privacy Act, and it would therefore

368 *Necessary and Desirable* 37–39, rec 6.

369 *Necessary and Desirable* 39–40, recs 7 and 8.

370 Bruce Slane, Privacy Commissioner *Report to the Minister of Justice in relation to the Parliamentary Service Bill* (2 November 1999).

be problematic to make parliamentary service bodies subject if that meant indirect access to documents prepared or held by members of Parliament. This is especially a consideration for the Parliamentary Service Commission which is made up of MPs. It is also an issue for the Parliamentary Service given that it employs the staff who actually work in MPs' offices.

Accordingly, it appears to me that the main desire for an exemption for the two parliamentary service bodies relates to the rights of access contained in principle 6 rather than any concern about the remaining 11 information privacy principles.

5.17 The Commissioner therefore recommended that both the Parliamentary Service Commission and the Parliamentary Service be made subject to all of the privacy principles except for principle 6. In addition, he recommended that the principle 6 right of access should apply to the Parliamentary Service in respect of its employees (as it does already) and that this should also be extended to cover prospective employees and contractors.[371] The Government Administration Committee's response to these recommendations in its report on the Parliamentary Service Bill was inconclusive, but the Committee stated that these issues would best be addressed when a general amendment to the Privacy Act is being considered.[372]

5.18 We believe that these matters are best considered together with the issues concerning the House of Representatives and MPs. We therefore propose that the Privacy Commissioner's recommendations with regard to the Parliamentary Service and the Parliamentary Service Commission should be considered by the same committee of Parliament that considers the application of the privacy principles to the House and MPs.

Q62 We propose that the issue of extending the privacy principles to the parliamentary service bodies should be reviewed by a committee of Parliament at the same time as that committee considers the application of the principles to the House of Representatives and MPs. Do you agree?

Ombudsmen

5.19 The Ombudsmen are excluded entirely from the definition of "agency". In *Necessary and Desirable*, the former Privacy Commissioner argued that there were three features of the Ombudsmen which might seem to warrant their exemption from the Privacy Act:

- their status as the review authority for Official Information Act (OIA) complaints;
- their status as officers of Parliament; and
- their status as a complaints body.

371 Bruce Slane, Privacy Commissioner *Report to the Minister of Justice in relation to the Parliamentary Service Bill* (2 November 1999); *1st supplement to Necessary and Desirable*, recs 7A and 8A.

372 Government Administration Committee *Report on the Parliamentary Service Bill* (2000) 10.

5.20 With regard to the first point, the Commissioner considered that, at most, the Ombudsmen's role as the review authority for OIA complaints might warrant a partial exemption from principle 6. This is already covered, the Commissioner argued, by section 55(d) of the Privacy Act, which provides that principles 6 and 7 do not apply to information in correspondence and communication between the Ombudsmen and any other agency in relation to investigations under the Ombudsmen Act, the OIA or the Local Government Official Information and Meetings Act.

5.21 On the second point, the Commissioner noted that the Auditor-General and the Parliamentary Commissioner for the Environment are not exempted from the Privacy Act, and that the Ombudsmen are subject to the Human Rights Act but not to the Privacy Act. The Commissioner did not consider that the Ombudsmen's status as officers of Parliament should place them outside the application of the privacy principles.

5.22 Regarding the third point, the Commissioner saw nothing inappropriate about a complaints body being subject to complaints to another complaints body, noting that, for example, the Privacy Commissioner can be the subject of complaints to the Ombudsmen and the Human Rights Commission. Making an institution subject to a complaints mechanism "does not undermine public confidence in it but rather strengthens it".

5.23 The Commissioner therefore recommended that the Ombudsmen should be made subject to the privacy principles. He noted that some overseas privacy laws expressly apply to ombudsmen.[373] We currently support the Commissioner's recommendation.

Q63 We propose that the Ombudsmen should be made subject to the privacy principles. Do you agree?

News media

5.24 "Agency" is defined as not including "in relation to its news activities, any news medium." "News activity" is defined to mean:

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

"News medium" is defined to mean "any agency whose business, or part of whose business, consists of a news activity; but, in relation to principles 6 and 7, does not include Radio New Zealand Limited or Television New Zealand Limited."

373 *Necessary and Desirable* 42–43, rec 10.

5.25 We believe the exclusion is justified. The free flow of information in the media is a crucial element of a free and democratic society. It is supported by section 14 of the New Zealand Bill of Rights Act 1990.[374] To require the media to comply with the privacy principles would be to impose an unreasonable limit on that freedom. It would not merely impede the media, but virtually hamstring it, to have to comply with, for example, principle 2 (personal information to be collected directly from the individual) and principle 11 (personal information not to be disclosed).

5.26 The Privacy Act is not unusual in granting the media or journalists an exemption from its provisions. So, for example, do the Fair Trading Act 1986,[375] the Financial Advisers Act 2008[376] and the various statutes regulating attendance at court proceedings.[377] Similar exceptions for media and journalism also exist in overseas privacy statutes.[378]

5.27 It is not as though the media are exempt from privacy laws and rules altogether: broadcasters are subject to the jurisdiction of the Broadcasting Standards Authority, and the print media to that of the Press Council. Those bodies can fashion principles appropriate to the media's special function. In addition, the media are potentially subject to the range of tortious and criminal liability that we have noted in Stage 3 of our Review. Moreover, the media do not fall outside the Privacy Commissioner's function of inquiring into, making statements about, and reporting on, matters affecting privacy.

"News activity"

5.28 While we believe that the news media exclusion should remain, there are questions about the way it is defined, and its confinement to the news media "in relation to its news activities." There has been debate about the meaning of "news activity". There are currently three possible interpretations:[379]

- That the media organisation is protected so long as it was acting in its capacity as a mass communicator, as opposed, for example, to its capacity as an employer (the "capacity" test).
- That the organisation is protected only so long as it is publishing news, or news-related material, which contains an element of public interest (the "public interest" test).
- That the organisation is protected only so long as it is publishing material within the genre of news and current affairs as opposed, say, to the genre of entertainment (the "genre" test).

374 Section 14 of the New Zealand Bill of Rights Act 1990 provides for the "right to freedom of expression, including the freedom to seek, receive and impart information and opinions of any kind in any form."

375 Fair Trading Act 1986, s 15.

376 Financial Advisors Act 2008, s 12(a).

377 For example, Criminal Justice Act 1985, s 138(3).

378 Privacy Act 1988 (Cth), s 7B(4); Data Protection Act 1998 (UK), s 32; Personal Information Protection and Electronic Documents Act SC 2000 c 5 (Canada), ss 4(2)(c), 7(1)(c).

379 See Elizabeth Paton-Simpson "The News Activity Exemption in the Privacy Act 1993" (2000) 6 NZBLQ 269.

5.29 Depending on which interpretation one favours, there could be an argument that, for example, a television reality show, or a humorous column in a newspaper, might fall outside the exemption. It is perhaps surprising that in the 16 years since the Act came into force there have been very few disputed instances. In those cases in which the definition of "news activity" has been at issue, the Privacy Commissioner (and the Tribunal) have taken a view quite generous to the media, holding for example that the *National Business Review*'s "Rich List"[380] and the television programme "Target"[381] are covered by the exemption. In such cases, of course, a failed complainant is not deprived of recourse: he or she can still complain to the Broadcasting Standards Authority, or, in the case of the print media, to the Press Council, although it is true that in the latter case there can be no substantive remedy such as damages.

5.30 The question is whether it would be possible to define "news activity" with any greater precision. Given the increasingly unclear line between news and entertainment, and the uncertain boundaries of even the term "news" itself, that would be a very difficult undertaking. Any formulation would still leave much to judgment in marginal cases. Our preferred position, therefore, is to leave the present wording as it is, and allow the Privacy Commissioner (and in appropriate cases the Tribunal) to make judgment calls on a case-by-case basis.

"News medium"

5.31 There is a further difficulty in determining the boundaries of the term "news medium". That is the difficulty of deciding how far it now extends beyond traditional broadcasters and print media to the array of alternative media: blogs and other websites, for instance. The problem manifests itself when one considers the avenues of complaint open to an individual whose privacy is infringed by publication of private information. If publication takes place in the print media, a complaint can be made to the Press Council. If it is in a broadcast, as that term is defined in the Broadcasting Act 1989,[382] the Broadcasting Standards Authority has jurisdiction over the matter. But many manifestations of the new media fall outside the sphere of both of these bodies. The question is whether complaints against these new media for breach of principle 11 can be investigated by the Privacy Commissioner. It will not be possible for the Commissioner to investigate if the websites or other media in question fall within the "news media" exception in section 2 of the Privacy Act. Most online publications (other than those associated with a print publication such as a newspaper or magazine, or with a broadcaster) would probably not fall within the news media exception because they are not in "business".[383] But there might be a few regular blogs or other online publications which, arguably, could be regarded as being "news media" within the definition in section 2. If that is so, there may be a few manifestations of the new electronic media which are not subject to any of the existing complaints jurisdictions – Press Council, Broadcasting Standards Authority, or Privacy Commissioner.

380 *Talley Family v National Business Review* (1997) 4 HRNZ 72.

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

382 See definitions of "broadcaster" and "broadcasting" in Broadcasting Act 1989, s 2(1).

383 There may be some argument about what "business" means in this context, however.

5.32 We wonder whether the definition of "news medium" should be amended to confine it in some way. On the one hand, this would avoid the possibilities of some publications, few though they might be, slipping through the net altogether. On the other, it might be argued that the privacy principles are simply not appropriate to any branch of the media. If it is considered desirable to restrict the meaning of "news medium", one option would be to confine it to print and broadcast media. However, this would mean that online versions of newspapers or broadcasts would be subject to complaints to the Privacy Commissioner unless a way could be found of excluding them. It would clearly be absurd if a person could not complain to the Privacy Commissioner about an article that appears in print, but could complain about the same article when it appears on a newspaper's website. An alternative option would be to provide in the Act that a news medium can only benefit from the Privacy Act exclusion if it is subject to a code of ethics and to a complaints procedure administered by an appropriate body (the Press Council, the Broadcasting Standards Authority, or any other relevant complaints body that might be established in future). The media exception in the Privacy Act 1988 (Cth) includes a provision somewhat along these lines.[384] We seek views on this matter.

Radio New Zealand and Television New Zealand

5.33 We have concerns about one further matter relating to the definition of "news medium". That is the subjection of Radio New Zealand Limited (RNZ) and Television New Zealand Limited (TVNZ) to principles 6 (access to personal information) and 7 (correction of personal information). Before the Privacy Act was passed, the OIA contained provisions enabling persons to access personal information about them held by agencies subject to that Act. Those access provisions, so far as they related to individuals, were removed to the Privacy Act in 1993. It was obviously felt that, as state broadcasters also subject to the OIA, RNZ and TVNZ were in a different position from other media. We wonder whether that distinction is justified. It is not just that the present provisions give private broadcasters an advantage over the state broadcasters in a very competitive market; subjection to the OIA can have that effect in other contexts too. It is rather that a requirement to allow access to, and correction of, personal information can have an effect – at the very least a delaying effect – on the dissemination of news. It might lead to an application for an injunction,[385] for example, or to lengthy stalling debate over whether information held is completely accurate. This might be regarded as an unjustified limitation on freedom of information whether the broadcaster be state or private. We wonder therefore whether the limiting reference to RNZ and TVNZ should be removed from the definition of "news medium" in section 2.[386] This would, of course, still preserve the right to access and correct information, such for example as employment information, which falls outside the "news activity" exemption. We acknowledge

384 Privacy Act 1988 (Cth), s 7B(4)(b).

385 Bearing in mind that access rights under principle 6 can be directly enforced in the courts where information held by a public sector agency is concerned: Privacy Act 1993, s 11(1). RNZ and TVNZ are public sector agencies in terms of the Act: Privacy Act 1993, s 2(1), definitions of "public sector agency" and "organisation"; Official Information Act 1982, sch 1.

386 This would also require a corresponding deletion of section 29(1)(g), which allows RNZ and TVNZ to withhold requested information if disclosure would be likely to reveal a journalist's source.

that an amendment of the kind we suggest would still leave differences between TVNZ and RNZ and the other media, because the state broadcasters would remain subject to the OIA with regard to information held by them.

Q64 We propose that the exclusion of the news media in relation to their news activities should remain in the Privacy Act. Do you agree?

Q65 We propose that the definition of "news activity" should remain as it is. Do you agree?

Q66 Do you think the definition of "news medium" should be amended to confine it to the print and broadcast media? Alternatively, should be it be confined to news media that are subject to a code of ethics and complaints procedure?

Q67 We propose that the limiting reference to Radio New Zealand and Television New Zealand should be removed from the definition of "news medium". Do you agree?

Q68 Are any other changes needed to the exclusions from the definition of "agency"?

SPECIFIC EXEMPTIONS IN PART 6 OF THE ACT

5.34 Part 6 of the Act provides for codes of practice (discussed in chapter 7), and for certain other types of specific exemption. Sections 54, 56 and 57 are discussed below. We are not aware of any issues in relation to section 55, which excludes certain types of information from the coverage of principles 6 and 7.

Q69 Are any changes needed to section 55?

Section 54 – authorisation by the Privacy Commissioner

5.35 Section 54 provides that the Privacy Commissioner may authorise an agency to collect, use or disclose information where this would otherwise breach principles 2, 10 or 11, if the Commissioner is satisfied that, "in the special circumstances of the case":

- the public interest outweighs any interference with the privacy of an individual that could result; or
- there is a "clear benefit to the individual concerned" that outweighs any interference with the privacy of the individual that could result.

The Commissioner may impose such conditions as he or she sees fit on such an authorisation. The Commissioner shall not grant an authorisation under section 54 if the person concerned has refused to authorise the collection, use or disclosure of his or her information for the relevant purpose.

5.36 The Commissioner has issued a Guidance Note to applicants seeking exemptions under section 54. The Commissioner's Annual Report includes a report on section 54 applications.[387] It seems that there are a few applications each year, but that many are not granted. A common reason for declining applications seems to be that the Commissioner considers that the exemption applied for is unnecessary, because the agency's objective can be achieved without breaching the privacy principles.

5.37 The reference to "the special circumstances of the case" would seem to mean that section 54 is not intended to allow for the granting of ongoing or generic exemptions. This is reinforced by the Commissioner's Guidance Note, which states:[388]

> Section 54 seems primarily designed for "one-off" situations. If the circumstances giving rise to an application are likely to arise again and again, or are a routine part of an agency's activities, it is likely that an exemption will be inappropriate. Consideration should instead be given to seeking a code of practice.

Should section 54 apply to other principles?

5.38 It is not clear why section 54 applies only to principles 2, 10 and 11. There may be instances in which exceptions to some other principles could be granted on the same basis. It would probably not be appropriate to allow exemptions to be granted in the case of principle 1, which is fundamental to the whole operation of the Act. It is also hard to see why exemptions should ever be allowed for principles 4, 5 and 8. In the *Necessary and Desirable* review, the Privacy Commissioner asked whether the Commissioner's power to grant exemptions under section 54 should be extended to principles 9 and 12, and finally recommended that the power be extended to principle 9 only.[389] We agree that the Commissioner should be able to grant exemptions from principle 9 under section 54.

Q70 We propose that section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principle 9. Do you agree? Should the Commissioner be allowed to grant exemptions under section 54 from any other principles?

Should section 54 be used for ongoing exemptions?

5.39 As noted above, OPC considers that section 54 is intended for "one-off" exemptions only. This seems consistent with the wording of the section, particularly the reference to "the special circumstances of the case". However, it has been suggested to the Law Commission that it should be possible to use section 54 to authorise ongoing collection, use or disclosure, rather than one-off exemptions only.

---

387 See for example Office of the Privacy Commissioner *Annual Report 2009* (Wellington, June 2009) 34.

388 Office of the Privacy Commissioner "Guidance Note to Applicants Seeking Exemption Under Section 54 of the Privacy Act" (1997) para 3.4.

389 Office of the Privacy Commissioner *Review of the Privacy Act 1993: Discussion Paper No 4: Codes of Practice and Exemptions* (Wellington, 1997) 7–8; *Necessary and Desirable* 219–220, rec 79.

5.40 Giving the Privacy Commissioner the power to authorise ongoing exemptions in some cases could be seen as a halfway house between one-off exemptions and the much more involved process of developing and approving a code of practice. It might be useful where a particular issue comes up again and again but is perhaps too specific to warrant the creation of a code.

5.41 However, the following cautionary points need to be considered in relation to the suggestion that the Privacy Commissioner could authorise ongoing exemptions under section 54:

- At present there is no evidence of a real problem. There is already quite a lot of flexibility in the privacy principles, and the experience with the existing provisions of section 54 suggests that many applications for ongoing exemptions would be turned down by the Privacy Commissioner on the grounds that what the agency seeks to do is already allowed under the Act.
- Giving the Commissioner the power to authorise ongoing exemptions would mean giving him or her significant powers to modify the terms of the Act. This is already true of the codes of practice provisions, but these include procedural safeguards relating to consultation and notification. Moreover, we propose in chapter 7 that codes of practice should be approved by Cabinet. Similar safeguards would surely need to be put in place for ongoing exemptions under section 54, in which case it is hard to see how they would differ from codes of practice.
- It is reasonably easy to see how ongoing exemptions could be justified on public interest grounds (section 54(1)(a)). Exemptions involving "a clear benefit to the individual concerned" (section 54(1)(b)) are a different matter, however. Subsection (1)(b) is more obviously suited to one-off applications relating to specific situations than to ongoing exemptions. It is likely to be difficult to assess the benefit to the individual where ongoing collection, use or disclosure is concerned. The same is probably true with regard to the provision in section 54(3) that an exemption shall not be authorised by the Commissioner where the individual concerned has refused to authorise the collection, use or disclosure. This provision seems to contemplate a one-off opportunity to refuse consent, and might be difficult to apply to an ongoing exemption.

5.42 For the reasons given in the above bullet points, we believe that the Privacy Commissioner should not be empowered to authorise ongoing exemptions under section 54.

Q71 We propose that section 54 should continue to be limited to one-off exemptions only. Do you agree?

Q72 Are any other changes needed to section 54?

Section 56 – personal, family or household affairs

5.43 Section 56 is deceptively short and simple. It provides that:

> Nothing in the information privacy principles applies in respect of—
>
> (a) The collection of personal information by an agency that is an individual; or
>
> (b) Personal information that is held by an agency that is an individual,—
>
> where that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs.

5.44 Most information privacy statutes in other countries have similar exemptions, although as discussed below there are some differences in the wording of the overseas provisions. The rationale of the exemption is clear enough – individuals should not have to comply with the Privacy Act in relation to everyday domestic activities such as taking photographs of friends and family or keeping records of family expenditure and activities. To routinely apply the Privacy Act to such activities would be both impractical and intrusive into people's personal and domestic lives. It could also see the Privacy Commissioner and the Human Rights Review Tribunal getting caught in the middle of domestic disputes. Nevertheless, the breadth of the exemption gives rise to significant concerns, particularly in the age of the internet, as discussed below.

5.45 The wording of section 56 refers only to information that is "collected or held" by an individual. In *S v P*, the Complaints Review Tribunal held that section 56 applies to use and disclosure of information, even though use and disclosure are not specifically referred to in the section:[390]

> [W]e accept the submissions of the Privacy Commissioner that the information privacy principles concern **collecting** (principles 1–4) and **holding** (principles 5–11) information. The **protection**, **use** or **disclosure** of information concern obligations that can only arise if an agency **holds** information. There is therefore no need for s. 56 to specifically refer to those obligations because they are covered by the use of the word **hold** in s. 56(b). Section 56, therefore, also covers the disclosure of information.

Meaning of "personal affairs"

5.46 Paul Roth has raised questions about the meaning of "personal affairs" in section 56.[391] He notes that this expression has been contentious in Australian freedom of information legislation, and that courts in Australia have veered between broad and narrow interpretations of "personal affairs". Roth asks, for example, whether information about a person's personal affairs can include information about his or her conduct at work? It could be desirable to clarify the meaning of "personal affairs", although we recognise that it would be quite difficult to do this. We note that the words "personal affairs" are also used in principle 4(b)(ii).

390 *S v P* (12 March 1998) Complaints Review Tribunal 3/98, 4.

391 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA56.5.

Q73 Should the meaning of "personal affairs" in section 56 be clarified? If so, how?

Scope of section 56

5.47 While there can be little doubt that an exemption along the lines of section 56 is necessary, it also creates a major gap in the protection offered by the Privacy Act. In our issues paper for Stage 3 of this Review we set out some hypothetical scenarios involving instances of surveillance. In relation to a number of these scenarios, we referred to the fact that a remedy might not be available through the Privacy Act because of section 56.[392] The question is whether the scope of section 56 can be narrowed while continuing to exclude the bulk of personal information collected or held in connection with personal, family or household affairs from the coverage of the privacy principles.

5.48 Some specific issues have been raised in relation to section 56. One concerns the use of section 56 where an individual has deliberately misled an agency, particularly in order to obtain information. For example, a person could obtain information about an individual by falsely claiming to be that individual or to have that individual's consent. At present a complaint could be brought about the agency's action in disclosing the information, but a complaint against the person who obtained the information under false pretences might well fail if that person could show that he or she obtained the information in connection with his or her personal or domestic affairs. Accordingly, the Privacy Commissioner recommended in *Necessary and Desirable* that section 56 should be amended so that an individual cannot rely on the domestic affairs exemption where that individual has collected personal information from an agency by falsely representing that he or she has the authorisation of the person concerned or is the person concerned.[393]

5.49 A second issue concerns the application of the section 56 exemption to activities that are unlawful. This issue has arisen in relation to intimate covert filming. At present there would be no remedy under the Privacy Act where, for example, a stepfather films his stepdaughter in the shower in a manner that would be in breach of the intimate covert filming provisions of the Crimes Act.[394] We understand that there have been cases of this sort. Prior to the release of the Law Commission's recommendations on intimate covert filming, the Privacy Commissioner recommended that the section 56 exemption should be limited so that it did not apply to intimate covert filming or to unlawful collection of personal information.[395] The Law Commission subsequently recommended that section 56 be amended to provide that the domestic affairs exemption does not

392 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP 14, Wellington, 2009) 224–234: see scenarios 1–4, 12, 15.

393 *Necessary and Desirable* 224–226, rec 82.

394 Crimes Act 1961, ss 216G, 216H.

395 *3rd supplement to Necessary and Desirable*, rec 82A.

extend to "information obtained through criminal offending whether or not [the respondent has been] charged or convicted".[396] The Commission saw the Privacy Act as the best vehicle for providing a civil remedy for intimate covert filming.

5.50 The two issues discussed above are comparatively straightforward. There are, however, a range of other situations in which the section 56 exemption seems problematic, but the solutions are by no means clear. Consider the following scenarios:

- A and B have been in a sexual relationship, in the course of which A has taken intimate photographs of B with her consent. When the relationship breaks up, A posts these photos on a publicly-accessible website without B's consent.
- C and D are university students who attend a wild party. C takes photographs of the party, which she puts on her page on a social networking site. One of the photographs shows D in a drunken and undignified state. The photographs are later seen by a prospective employer, and D is not employed as a result.
- E writes a blog, much of which is concerned with her everyday life and her interactions with friends and family. She mentions in the blog that a friend is having an affair. Although she does not name the friend, his identity is apparent from the context to those who know him.

In each of these cases, it is likely that the individual who has (arguably) breached another person's privacy could successfully use the section 56 exemption.

5.51 Each of these scenarios also involves information being made available online. Although the issues concerning section 56 do not arise only from the internet, the internet does create new problems when material relating to "personal, family or household affairs" is made available to a much wider audience. It is arguable that making the material more widely available by placing it on the internet takes it out of the personal, family or household sphere, but this is by no means clear, particularly if access to the site in question is restricted to some degree. For an increasing number of people, websites are the modern equivalents of diaries or family photo albums.

5.52 It may be that there is no realistic way of restricting the scope of section 56 without rendering it ineffective. A recent article on data protection laws and online social networking by Gehan Gunasekara and Alan Toy argues that the section 56 exemption should be given a fairly wide reading and that an individual's motives for collecting, using or disclosing information should not affect that individual's ability to rely on this exemption.[397]

5.53 If it is considered desirable to restrict the scope of section 56, one option would be to modify the wording of the section. Section 56 refers to personal information that is held "*solely or principally* for the purposes of, or in connection with" a person's personal, family or household affairs. By contrast, overseas statutes use phrases like:

396 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) 37.

397 Gehan Gunasekara and Alan Toy "'MySpace' or Public Space: The Relevance of Data Protection Laws to Online Social Networking" (2008) 23 NZULR 191, 213.

- "*only* for the purposes of";[398]
- "*only* for the purposes of, or in connection with";[399]
- "personal information that the individual collects, uses or discloses for personal or domestic purposes *and does not collect, use or disclose for any other purpose*";[400]
- "*concerned only with the management of* his personal, family or household affairs";[401] and
- "in the course of a *purely* personal or household activity".[402]

Thus, overseas legislation seems to be more tightly confined to collection, use or disclosure that is only for personal, household or family purposes and for no other purposes.

5.54 A second approach would be to expressly exclude certain matters from the coverage of section 56 (as with the proposals discussed above to exclude misleading or criminal conduct). For example, the statute could provide that section 56 does not apply where:

- The person collecting, using or disclosing personal information knows that the person to whom that information relates has refused consent for such collection, use or disclosure. The person concerned would probably have to clearly indicate a refusal of consent, and there would not be a positive onus on the person collecting, using or disclosing the information to seek consent.
- The person collecting, using or disclosing the information has malicious motives for doing so.
- The person collecting, using or disclosing the information does so at least in part in order to obtain some financial benefit.
- The collection, use or disclosure is "highly offensive", or causes harm in one of the forms referred to in section 66(1)(b) of the Act.

Such amendments might help to deal with some problematic cases. However, they might still not assist in, for example, the case of a person posting embarrassing photographs of another on a social networking site, unless a malicious motive, a refusal of consent, or identifiable harm could be demonstrated.

5.55 A third, and more far-reaching option, would be not to treat personal, family and household affairs purposes as an exemption. Instead, the Commissioner and the Tribunal could be required to give due weight, in dealing with complaints against individuals, to the fact that the information in question was collected or held for the purposes of personal, family or household affairs. This would essentially mean balancing the privacy interests of the individual to whom the information relates against the interests of other individuals in the autonomous management of their personal and domestic affairs. Individuals would become subject to the privacy principles even in relation to their personal and domestic

398 Data Protection Act 1998 (UK), s 36.

399 Privacy Act 1988 (Cth), s 16E.

400 Personal Information Protection and Electronic Documents Act SC 2000 c 5, s 4(2)(b).

401 Personal Data (Privacy) Ordinance (Hong Kong), s 52(a).

402 European Union Directive 95/46/EC, art 3(2).

affairs, but they would be given a significant amount of leeway in complaints. The Privacy Commissioner could also issue guidelines to assist individuals in understanding how the Privacy Act applies to them. Such a change might, nonetheless, give rise to significant uncertainty, and leave the Privacy Commissioner and the Tribunal having to make some very difficult judgements.

5.56 We propose that the section 56 exemption should not apply where information is obtained by misleading or unlawful conduct. With regard to the wider issues about the scope of section 56, our preliminary view is that the section 56 exemption should not apply where the actions of the person seeking to rely on the exemption cause harm to another person or persons. Harm could be defined in the terms currently set out in section 66(1)(b) of the Act. In chapter 8 we propose to remove the harm threshold for complaints. If the proposal to remove the harm threshold results in the deletion of section 66(1)(b), the wording of that provision could be included (with necessary modifications) in section 56.

Q74 We propose that section 56 should be amended to provide that it does not apply where a person has collected information from an agency by engaging in misleading conduct (in particular, by falsely claiming to have the authorisation of the individual to whom the information relates or to be that individual). Do you agree?

Q75 We propose that section 56 should be amended so that it does not apply where personal information is obtained unlawfully (whether or not the person obtaining the information has been charged or convicted of a criminal offence). Do you agree?

Q76 We propose that section 56 should be amended so that it does not apply where the collection, use or disclosure of personal information results in identifiable harm to another individual. Do you agree? If not, do you support any of the other options discussed in paragraphs 5.53–5.55?

Q77 Do you have any other suggestions for amending section 56?

Section 57– intelligence agencies

5.57 Section 57 provides that principles 1 to 5 and 8 to 11 do not apply to information collected, held, obtained, used or disclosed by, or disclosed to, an intelligence organisation. In other words, only the access, correction and unique identifier principles apply to these organisations. Section 2 defines "intelligence organisation" as meaning the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB).

5.58 Section 57 and other special provisions in relation to the intelligence organisations (discussed below) recognise the unique nature of the work of the security and intelligence agencies. Some of the distinctive features of their work have been summarised by the NZSIS:[403]

- Security investigations are long-term and do not always have a clear end point, in contrast to law enforcement investigations which typically end with the laying of charges.
- Security investigations are "prospective in nature, with the primary emphasis on prevention".
- Intelligence is collected covertly from human sources and by means of surveillance devices.

The exemptions in the Privacy Act in relation to the intelligence organisations allow them to continue to operate covertly and to protect their sources and methods.

5.59 At the same time, the work of the intelligence organisations clearly has significant implications for privacy, which is why they are not exempted entirely from the Act and why they are subject to oversight not only by the Privacy Commissioner but also by the Inspector-General of Intelligence and Security (as discussed below). The Privacy Commissioner's view is that:[404]

- the intelligence organisations' roles should be restricted to a tight brief and should not "stray into areas which can be appropriately managed by normal and open governmental and policing activities";
- while much of the organisations' work will need to be conducted in secret, there will be areas in which information can be disclosed publicly, to the individuals concerned or to oversight bodies;
- the organisations should be subject to similar accountability mechanisms to other agencies (albeit sometimes in a modified manner), except where there is a good reason for this not to occur; and
- where the organisations unjustifiably breach individual rights, including the right to privacy, redress should be available.

403 New Zealand Security Intelligence Service "Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS" www.nzsis.govt.nz (accessed 19 January 2010) paras 8–12.

404 *Necessary and Desirable* 224. The current Privacy Commissioner takes the same view: see Marie Shroff "Linking Intelligence to Provide Value: Personal Information, Privacy and the Information Century" (speech to Institute of Intelligence Professionals Conference, Wellington, 25 August 2009).

Access requests and use of the "neither confirm nor deny" response

5.60 Section 27 of the Privacy Act allows information requested pursuant to principle 6 to be withheld if disclosure of the information would be likely to prejudice the security or defence of New Zealand, the maintenance of the law, and other related interests. Section 32 provides that, where an access request pursuant to principle 6 relates to information to which section 27 "applies, or would, if it existed, apply", and where the interest protected by section 27 would be prejudiced if the existence or non-existence of the information were to be disclosed, the agency responding to the request may give written notice to the applicant that it neither confirms nor denies the existence or non-existence of that information.

5.61 The NZSIS often relies on the ability to neither confirm nor deny under section 32, and has set out its reasons for doing so. It explains that "a request for information to the NZSIS is tantamount to asking whether there is or has been an investigation by the NZSIS into the individual or the subject matter." Furthermore, neither confirming nor denying the existence or non-existence of information may be necessary to avoid disclosing the existence of a covert source. While it might seem that there would be no harm in confirming that no information is held, the NZSIS maintains that confirming the non-existence of information can prejudice security by disclosing what the Service does not know or is not investigating.[405] In particular, it states that:[406]

- Not knowing whether the NZSIS is investigating a particular activity or not has something of a deterrent effect. If it becomes a simple exercise to identify what is not of interest to the NZSIS, the benefit of the deterrent effect is lost.
- If a correspondent is undertaking activities of security concern, and receives a "no information held" response for a subject they believed should be under investigation, they now know they have not been detected.

Processes for privacy complaints against the intelligence organisations

5.62 Section 81 of the Privacy Act sets out a special procedure relating to privacy complaints against the intelligence organisations (bearing in mind that these can only be complaints of breaches of principles 6, 7 or 12). Where, after investigating a complaint against an intelligence organisation, the Privacy Commissioner considers that there appears to have been an interference with the privacy of an individual, the Commissioner shall report that opinion, and the reasons for it, to the relevant intelligence organisation. The Commissioner may also make recommendations, and may request that the organisation report to the Commissioner within a reasonable time on the steps (if any) that it proposes to take to comply with the Commissioner's recommendations. If, within a reasonable time after receiving that report, the Commissioner considers that the organisation has not taken adequate steps to address the issue, the Commissioner may send a copy of the report and recommendations to the Prime Minister, who may lay part or all of the report before the House of Representatives. Section 81(6) provides that sections 76 and 77 (concerning

405 New Zealand Security Intelligence Service "Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS" www.nzsis.govt.nz (accessed 19 January 2010) paras 13–18.

406 New Zealand Security Intelligence Service "Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS" www.nzsis.govt.nz (accessed 19 January 2010) para 19.

compulsory conferences and procedures following the Privacy Commissioner's investigation of a complaint), and all of the sections concerning proceedings before the Human Rights Review Tribunal, do not apply to complaints against intelligence organisations. In other words, complaints against intelligence organisations cannot proceed to the Tribunal.

5.63 In parallel with the above procedures, people can also complain about breaches of privacy by intelligence organisations to the Inspector-General of Intelligence and Security. The functions of the Inspector-General include inquiring on his or her own motion, or at the request of the Minister, into any matter that relates to compliance by intelligence agencies with the law; and inquiring into any complaint by a New Zealander concerning an act or omission of an intelligence agency that may have adversely affected the complainant.[407] This would seem to allow the Inspector-General to investigate privacy matters that go beyond those that can be investigated by the Privacy Commissioner – for example, the Inspector-General could investigate a complaint that a person has been adversely affected by a disclosure of personal information by an intelligence organisation. The Inspector-General may consult with the Privacy Commissioner in relation to any matter relating to the Inspector-General's functions, and likewise the Privacy Commissioner may refer complaints to the Inspector-General and consult with the Inspector-General.[408]

Extending other privacy principles to the intelligence organisations

5.64 In *Necessary and Desirable*, the Privacy Commissioner recommended that the exemption in section 57 should be narrowed so that principles 1, 5, 8 and 9 apply to the intelligence organisations.[409] The Commissioner was of the view that these principles "provide a sound basis for fair information handling and have clear relevance to intelligence organisations", and that they would not need to be amended to establish any national security exception.[410] Submissions were overwhelmingly in favour of applying these principles to the intelligence organisations. The NZSIS and the GCSB had no objections to an amendment to the Privacy Act to make them subject to principles 1, 5, 8 and 9. The two intelligence organisations did enter a caveat with regard to principle 9, noting that it is often necessary to retain intelligence information for future purposes. They did not, however, appear to be arguing for an amendment or exception to principle 9, but rather for flexibility in its application to intelligence organisations. The NZSIS and GCSB also expressed a preference for oversight of compliance with these principles to be carried out by the Inspector-General rather than the Privacy Commissioner. The intelligence organisations made clear in their submissions that they considered it essential that they continue to be exempted from principles 2, 3, 4, 10 and 11.[411]

---

407 Inspector-General of Intelligence and Security Act 1996, s 11(1)(a) and (b).

408 Inspector-General of Intelligence and Security Act 1996, s 12(2); Privacy Act 1993, ss 72B, 117B. Section 15(3) of the Inspector-General of Intelligence and Security Act 1996 provides that nothing in section 12 of that Act limits the powers, duties and responsibilities of the Privacy Commissioner.

409 *Necessary and Desirable* 224–229, rec 83.

410 *Necessary and Desirable* 226.

411 New Zealand Security Intelligence Service, submission to the Office of the Privacy Commissioner, 2 December 1997; Government Security Communications Bureau, submission to the Office of the Privacy Commissioner, 31 October 1997.

Q78 Should principles 1, 5, 8 and 9 apply to the intelligence organisations?

Q79 Should there be any other changes to the exemption for the intelligence organisations under section 57?

Q80 Should there be any changes to the procedures for investigating privacy complaints involving the intelligence organisations? Are any problems created by the dual jurisdiction of the Privacy Commissioner and the Inspector-General of Intelligence and Security?

POSSIBLE NEW EXEMPTIONS

5.65 The Law Commission is not aware of a need for any new exemptions to be included in the Act, but submitters are welcome to propose new exemptions.

Q81 Should any new exemptions be included in the Privacy Act?

Chapter 6
Privacy Commissioner

6.1 In this chapter we review the Privacy Commissioner's existing role, functions and powers, explain how they work in practice and present options for reform.

6.2 The Commissioner exercises her functions with the assistance of her staff. In this chapter, therefore, we refer to the Privacy Commissioner ("the Commissioner") and the Office of the Privacy Commissioner ("the Office" or "OPC") interchangeably.

OVERVIEW OF COMMISSIONER'S ROLE, FUNCTIONS AND POWERS

6.3 The Commissioner has extensive functions under the Privacy Act and also has some functions under other enactments. We outline the functions below, grouped into three categories: functions in section 13, elsewhere in the Act, and under other enactments.

Functions under section 13

6.4 The Commissioner's functions under this section cover fully three pages of the statute book. Rather than try to summarise them, we set out section 13 of the Act:

> (1) The functions of the Commissioner shall be –
>
> (a) to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles:
>
> (b) when requested to do so by an agency, to conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles:
>
> (c) to monitor the use of unique identifiers, and to report to the Prime Minister from time to time on the results of that monitoring, including any recommendation relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of the individual:
>
> (d) to maintain, and to publish, in accordance with section 21, directories of personal information:
>
> (e) to monitor compliance with the public register privacy principles, to review those principles from time to time with particular regard to Council of Europe Recommendations on Communication to Third Parties of Personal Data Held by Public Bodies (Recommendation R (91) 10), and to report to the responsible Minister from time to time on the need for or desirability of amending those principles:

(f) to examine any proposed legislation that makes provision for –

(i) the collection of personal information by any public sector agency; or

(ii) the disclosure of personal information by one public sector agency to any other public sector agency, –

or both; to have particular regard, in the course of that examination, to the matters set out in section 98, in any case where the Commissioner considers that the information might be used for the purposes of an information matching programme; and to report to the responsible Minister the result of that examination:

(g) for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner:

(h) to make public statements in relation to any matter affecting the privacy of the individual or of any class of individuals:

(i) to receive and invite representations from members of the public on any matter affecting the privacy of the individual or of any class of individuals:

(j) to consult and co-operate with other persons and bodies concerned with the privacy of the individual:

(k) to make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interests of the privacy of the individual:

(l) to provide advice (with or without a request) to a Minister or an agency on any matter relevant to the operation of this Act:

(m)to inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby:

(n) to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring:

(o) to examine any proposed legislation (including subordinate legislation) or proposed policy of the Government that the Commissioner considers may affect the privacy of individuals, and to report to the responsible Minister the results of that examination:

(p) to report (with or without request) to the Prime Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of the individual:

(q) to report to the Prime Minister from time to time on the desirability of the acceptance, by New Zealand, of any international instrument relating to the privacy of the individual:

(r) to report to the Prime Minister on any other matter relating to privacy that, in the Commissioner's opinion, should be drawn to the Prime Minister's attention:

(s) to gather such information as in the Commissioner's opinion will assist the Commissioner in carrying out the Commissioner's functions under this Act:

(t) to do anything incidental or conducive to the performance of any of the preceding functions:

(u) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

(1A) Except as expressly provided otherwise in this or another Act, the Commissioner must act independently in performing his or her statutory functions and duties, and exercising his or her statutory powers, under –

(a) this Act; and

(b) any other Act that expressly provides for the functions, powers, or duties of the Commissioner (other than the Crown Entities Act 2004).

(2) The Commissioner may from time to time, in the public interest or in the interests of any person or body of persons, publish reports relating generally to the exercise of the Commissioner's functions under this Act or to any case or cases investigated by the Commissioner, whether or not the matters to be dealt with in any such report have been the subject of a report to the responsible Minister or the Prime Minister.

Functions and powers elsewhere in Privacy Act

6.5 In addition to section 13, a number of other sections of the Act confer functions and powers on the Commissioner. Some of the Commissioner's most significant functions, such as receiving complaints, are in fact not specifically listed in section 13.

6.6 Section 14 is important as it sets out certain matters that the Commissioner must have regard to in exercising his or her functions and powers. The Commissioner must have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of Government and business to achieve their objectives in an efficient way. He or she must also take account of international obligations accepted by New Zealand and consider any developing general international guidelines relevant to the better protection of individual privacy. Finally, the Commissioner is instructed to have due regard to the information privacy principles and the public register privacy principles contained in the Act.[412]

6.7 If the Commissioner thinks it would be desirable to obtain a declaratory judgment from the High Court in accordance with the Declaratory Judgments Act 1908, he or she can refer the matter to the Director of Human Rights Proceedings for the purpose of deciding whether proceedings under that Act should be instituted.[413]

6.8 The Commissioner is also empowered to publish directories of personal information that include the nature of personal information held by any agency; the purpose to which any personal information is held by any agency; the classes of individuals about whom personal information is held by any agency; and a number of other related matters.[414] The Commissioner may require agencies to supply information for the purpose of the publication of these directories.[415]

412 Privacy Act 1993, s 14.

413 Privacy Act 1993, s 20.

414 Privacy Act 1993, s 21.

415 Privacy Act 1993, s 22.

6.9 The Commissioner must also review the operation of the Act every five years,[416] and has made a great many recommendations under this provision.[417]

6.10 Section 36 gives the Commissioner power to authorise a public sector agency to charge for access to and correction of personal information.

6.11 Section 61 of the Act gives the Commissioner power, on a complaint made by any person or on the Commissioner's own initiative, to inquire into any public register provision if it appears to the Commissioner that the provision is inconsistent with any of the information privacy principles or public register privacy principles.

6.12 Section 63 of the Act enables the Commissioner to issue codes of practice in relation to public registers.

6.13 The Commissioner is similarly empowered under Part 6 of the Act to issue codes of practice that modify the application of any one or more of the privacy principles in relation to a particular type of information, agency, activity or industry. These codes of practice are important since they constitute law and are binding, so there are a number of provisions requiring the Commissioner to make clear what is being proposed and to secure comment on it before the code is issued. Failure to comply with a code is treated as if it is a breach of a privacy principle.[418]

6.14 The Commissioner may also authorise collection, use or disclosure of personal information that would otherwise breach principles 2, 10 or 11 if he or she believes that the public interest in the action outweighs the potential privacy interference, or that the action involves a clear benefit to the individual that outweighs the privacy interference.[419]

6.15 Part 8 of the Act gives the Commissioner jurisdiction to deal with individual complaints.

6.16 The Commissioner also has a role to perform in information matching under Part 10 of the Act.

6.17 We discuss codes of practice in chapter 7, complaints in chapter 8, and information matching in chapter 9 of this paper. The rest of this chapter therefore does not deal with the Commissioner's role in relation to these aspects of the Act in any detail. We have previously proposed reforms to the public register provisions of the Act,[420] so we do not discuss the Commissioner's role in relation to public registers here.

416 Privacy Act 1993, s 26.

417 *Necessary and Desirable* and supplements.

418 Privacy Act 1993, s 53.

419 Privacy Act 1993, s 54.

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

Functions under other enactments

6.18 The Commissioner also has quite a large number of miscellaneous functions conferred under other enactments. These usually involve providing specialist input on privacy matters or some form of safeguard or oversight role. Some give the Commissioner a review or complaints-handling function. These functions can be broadly divided into the following categories:

- complaints investigation;[421]
- scrutiny or approval of information-disclosure arrangements;[422]
- consultations on complaints handled by other agencies;[423]
- appointment to other bodies;[424]
- codes of practice;[425] and
- information matching.[426]

HOW THE FUNCTIONS ARE EXERCISED IN PRACTICE

6.19 This section describes the way in which the Commissioner's functions are carried out in practice. We outline the OPC's activities under each of its statutory functions below.

Functions under section 13

Section 13(1)(a) – to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles

6.20 The Commissioner carries out a wide range of activities under this function, including meeting with opinion leaders, the news media, government, business leaders and civil society groups; providing training programmes for agencies; answering media enquiries, making statements and media releases; maintaining a website (www.privacy.org.nz); making public speeches; conducting a privacy issues forum at least every two years; and producing written educational materials.[427]

421 Health Act 1956, s 22F; Domestic Violence Act 1995, ss 118–120 and Domestic Violence (Public Register) Regulations 1996, reg 11; Social Security Act 1964, ss 11B and 131F; Adoption (Intercountry) Act 1997, s 13.

422 Passports Act 1992, s 36.

423 Official Information Act 1982, s 29B; Local Government Official Information and Meetings Act 1987, s 29A; Health and Disability Commissioner Act 1994, ss 19, 21, 23 and 40; Customs and Excise Act 1996, s 281; Financial Transactions Reporting Act 1996, s 25; Social Security Act 1964, s 11B; Ombudsmen Act 1975, s 17A; Inspector-General of Intelligence and Security Act 1996, s 12; Corrections Act 2004, s 182D.

424 Currently none. Formerly Human Rights Act 1993, s 7.

425 Dog Control Act 1996, s 35 (additional powers in making codes affecting dog registers); Domestic Violence Act 1995, ss 122–124 (powers to prescribe aspects of regime governing non-publication of information relating to protected persons on public registers).

426 Social Security Act 1964, ss 11A and 131G; Education Act 1989, ss 226A and 238B.

427 See, eg, regular newsletter entitled *Private Word*; case notes on complaints; Office of the Privacy Commissioner *On the Record: Privacy Impact Assessment Handbook* (Wellington, 2007); *Health Information Check-up* (Wellington, 2008); *Good Privacy is Good Business* (Wellington, 2008). The Office also contributes to other publications. See, eg, Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2007) Chapter 15: Privacy and Fair Handling of Personal Information.

Section 13(1)(b) – when requested to do so by an agency, to conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles

6.21 This function has not been exercised by the office because no agencies have asked to be audited.

Section 13(1)(c) – to monitor the use of unique identifiers, and to report to the Prime Minister from time to time on the results of that monitoring, including any recommendation relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of the individual

6.22 The OPC has conducted extensive work on unique identifiers, including considering particular issues such as the National Health Index Number, occasional policy work on Bills, examining cases for relaxation or prohibition on shared unique identifiers in particular cases, granting exemptions under codes of practice and scrutinising the use of unique identifiers in government data matching.

Section 13(1)(d) – to maintain, and to publish, in accordance with section 21, directories of personal information

6.23 This function has not been exercised.

Section 13(1)(e) – to monitor compliance with the Public Register Privacy Principles and to review those principles from time to time

6.24 The office does significant work in the policy area when public registers are proposed or set up. As noted above, the Law Commission has reported separately on public registers,[428] so we do not propose to deal with these issues again here.

Section 13(1)(f) – to examine any proposed legislation that makes provision for the collection of personal information by any public sector agency; or the disclosure of personal information by one public sector agency to any other public sector agency, or both

6.25 Under this provision the OPC examines all proposed legislation regarding information matching and engages with the agencies involved to ensure that the Privacy Act aspects of the proposal are properly provided for. As part of the assessment process the OPC has developed requirements for information matching privacy impact assessments. The OPC reports to the relevant Minister or select committee as necessary.

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

Section 13(1)(g) – for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner

6.26 Under this function the OPC runs around 70 standardised and tailored training programmes each year, for a wide range of agencies, on topics including the Privacy Act, the Health Information Privacy Code, Mental Health and Privacy, and Information Matching.

Section 13(1)(h) – to make public statements in relation to any matter affecting the privacy of the individual or any class of individuals

6.27 The OPC makes public statements on privacy and related matters through a variety of channels including media responses, statements, media releases, articles and publications on subjects of topical interest that fall within the Privacy Act. Furthermore, the office makes submissions to select committees, makes speeches, publishes its regular newsletter and puts materials on its website. The OPC networks and is represented at meetings and conferences.

Section 13(1)(i) – to receive and invite representations from members of the public on any matter affecting the privacy of the individual or of any class of individuals

6.28 The OPC receives 6000 calls annually on its enquiries line. The office also receives extensive correspondence. Many suggestions and representations are made at public conferences, educational seminars and speaking engagements where the Commissioner and staff speak or present papers. From time to time the office actively solicits representations, for example, in relation to discussion papers for the periodic review of the operation of the Act under section 26, and in developing guidelines and codes of practice.

Section 13(1)(j) – to consult and co-operate with other persons and bodies concerned with the privacy of the individual

6.29 The OPC has active networks with Privacy Commissioners working in other jurisdictions and co-operates with international organisations working in privacy, including APEC, the OECD and the International Organisation for Standardisation. Within New Zealand the OPC has regular contact with various bodies that have complaints functions involving privacy, in particular the Office of the Ombudsmen and the Health and Disability Commissioner. The office also liaises with many other organisations whose work touches upon privacy.

Section 13(1)(k) – to make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interests of the privacy of the individual

6.30 The Commissioner executes this function in many different contexts. These include the complaints and investigation process (for example, the Commissioner often suggests specific changes to agency processes as a result of complaints). They also include the OPC's work on generic issues to improve privacy practices within agencies (for example, calling on Chief Executives to urge change). As well, this function involves ongoing work in the policy area and in the monitoring of information matching programmes.

Section 13(1)(l) – to provide advice (with or without request) to a Minister or an agency on any matter relevant to the operation of the Act

6.31 As with the previous function, this function is exercised in many different contexts. For example, enquiries, complaints and approaches from agencies may result in providing advice. There is significant consultation with private sector agencies about current or proposed practices. Meetings with private sector chief executives and government departments, and education and speaking engagements, are often opportunities to provide advice.

Section 13(1)(m) – to inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby

6.32 Past examples of such enquiries include the *Kaitiaki Nursing New Zealand* enquiry in 2007, and the Guthrie Card, Canterbury DHB patient notes and Rawhiti Trust Hospital Board enquiries, all in 2003. On occasion the OPC writes directly to an agency to ask for an explanation of an incident or event, or an announced product or policy, if it appears that individuals' privacy has been compromised.

Section 13(1)(n) – to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring

6.33 The office has a technology team that monitors technological developments and media reports, builds contacts and conducts environmental scans that are incorporated into the policy work of OPC.

6.34 Other activities under this function include commissioning regular public opinion surveys to evaluate public attitudes to privacy and technological developments, and participating in the work of the International Working Group on Data Protection and Telecommunications and the OECD Working Party on Information Security and Privacy. The OPC also occasionally commissions expert reports into technological issues.

Section 13(1)(o) – to examine any proposed legislation (including subordinate legislation) or proposed policy of the Government that the Commissioner considers may affect the privacy of individuals, and to report to the responsible Minister the results of that examination

6.35 This is a major activity of the office. The OPC is consulted at various stages on all public sector policy and legislation developments that may have privacy impacts.[429] In the 2007–2008 financial year the legal and policy team contributed to 260 policy and legislative projects.[430] The Office also reviews all Bills introduced

429 Departments are required to consult the OPC on cabinet papers: CabGuide http://cabguide.cabinetoffice.govt.nz/procedures/consultation/inter-agency-consultation (accessed 31 July 2009).

430 Office of the Privacy Commissioner *Annual Report of the Privacy Commissioner 2008* (Wellington, 2008) 34. No figure is available for the 2008–2009 financial year.

into the House for privacy impacts since the Commissioner is not consulted on all Bills prior to their introduction. The office has submitted more than 80 formal reports to the Minister since 1993.

Section 13(1)(p) – to report (with or without request) to the Prime Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of the individual

6.36 This function has not been explicitly exercised. On one occasion a report was prepared but was not ultimately submitted. However, the Office believes that having this power is helpful as a "reserve power" to be exercised only sparingly, but a necessary lever to secure voluntary compliance.

Section 13(1)(q) – to report to the Prime Minister from time to time on the desirability of the acceptance, by New Zealand, of any international instrument relating to the privacy of the individual

6.37 This function has not been exercised because there has been no formal international instrument that would call for such a report since the Privacy Act was enacted.

Section 13(1)(r) – to report to the Prime Minister on any other matter relating to privacy that, in the Commissioner's opinion, should be drawn to the Prime Minister's attention

6.38 This function has not been explicitly exercised. Again, however, the Office views this as a "reserve power" that is useful in securing voluntary compliance with the Act.

Section 13(1)(s) – to gather such information as in the Commissioner's opinion will assist the Commissioner in carrying out the Commissioner's functions under this Act

6.39 Information is gathered to assist in the carrying out of the Commissioner's functions from a wide variety of sources, including the OPC's specialist privacy library, monitoring of and research into technology and developments, the news media, liaison with agencies, interactions with the public through the Office's public enquiries line, public opinion surveys and conferences, international meetings and networks.

Section 13(1)(u) – to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

6.40 Many of the core functions of the OPC's work are actually found elsewhere in the Act, rather than in section 13. These are outlined in paragraphs 6.5 to 6.16. As described in paragraph 6.18, the Commissioner also has functions under other enactments.

Other functions

6.41 Many of the Commissioner's activities in relation to her other functions are described in other chapters of this paper. Therefore we only discuss here activities that are not described elsewhere.

Section 20 – declaratory judgments

6.42 This function has not been exercised, although it has been considered on a number of occasions. In fact, the Commissioner or Director of Human Rights Proceedings could seek a declaratory judgment without this specific authorisation in the Privacy Act, as the Declaratory Judgments Act 1908 allows anyone to do so.[431]

Section 22(b) – requiring agencies to supply information

6.43 The Commissioner often requests agencies to explain actions they have taken. This function is also used in relation to the work performed by enquiries officers.

Section 36 – authorising agency to charge

6.44 The Commissioner has received a small number of requests for authorisation to charge for access to and correction of personal information. Some authorisations have been granted.

TITLE AND PLACEMENT OF SECTION 13

6.45 So, long though section 13 is, it contains by no means all the Privacy Commissioner's functions. Its current title, along with its position early in the Act, could mislead a person coming to the Act for the first time into believing that it contains an exhaustive list. There may be merit in expressly indicating in it that the functions conferred by it are in addition to those conferred by other provisions, and its section heading might be amended to read "Further functions". Consideration might also be given to locating it later in the Act.

Q82 Should section 13, or its heading, indicate that it is not an exhaustive list of the Privacy Commissioner's functions? Where should section 13 be located in the Act?

431 Declaratory Judgments Act 1908, s 3. Note, however, that codes of practice may not be covered by this section as they are not regulations.

SHOULD THE COMMISSIONER'S FUNCTIONS BE CONFINED TO THOSE RELATING TO INFORMATION PRIVACY?

6.46 The Privacy Act is primarily concerned with the privacy of personal information. However, some of the Commissioner's functions go beyond this in that they relate to the protection of individual privacy more generally.[432] Some of these were transferred from the Human Rights Commission to the Privacy Commissioner at the inception of the office in 1991. The Human Rights Commission jurisdiction related to privacy in a general sense, not only privacy of personal information.[433] It had a "watchdog" role which has now been inherited by the Privacy Commissioner. In contrast to this general remit, some of the Commissioner's core functions, such as complaints, are confined to the information privacy principles, codes of practice and information matching.

6.47 A question therefore arises whether these wider functions are appropriate, or whether the Commissioner's functions ought to be more tightly focussed on privacy of personal information, in line with the rest of the Act. In discussing these wider functions, we are referring to sections 13(1)(g), 13(1)(h), 13(1)(i), 13(1)(j), 13(1)(k), 13(1)(m), 13(1)(n), 13(1)(o), 13(1)(p), 13(1)(q) and 13(1)(r). The potential difficulty with the wide scope of these is that privacy is an inherently vague concept in the abstract. There are many competing definitions of it and many different ways of thinking about it. It is an elusive and protean concept.[434] Some may be concerned, therefore, that it is not clear what empowering the Commissioner to look at privacy generally involves.

6.48 To this end, it may be thought that there are problems in defining the functions of a public agency by reference to the concept of privacy, the precise boundaries of which are not clear. It is always best with legislation to target with some precision the mischief that a statute aims to address. There are many different mischiefs that cause privacy to be invaded. Many of them are dealt with by other aspects of the law. It is not clear that they should be dealt with under such general provisions, rather than by specific, targeted legislation.

6.49 It might also be argued that the Privacy Commissioner may be more effective if she concentrates on the core responsibilities of data protection than if she ranges much more broadly.

6.50 On the other hand, it could be said that to split the various aspects of privacy is not helpful and may be artificial. It may be seen as artificial to draw a distinction between informational and spatial privacy, so confining the Commissioner's functions to informational privacy. This may cause practical difficulties, too, in determining what is and is not within the proper scope of the Commissioner's role. In our report for stage 3 of this review, we recommend that the Privacy Commissioner have extended functions in relation to monitoring surveillance.[435] In chapter 13 of this issues paper we ask whether she should have further powers in relation to technological developments.

---

432 Privacy Act 1993, ss 13(g)-(k) and (m)-(r).

433 Human Rights Commission Act 1977, Part 5.

434 See further New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008), and in particular Chapters 2 and 3, for extensive discussion of competing theories of privacy and its conceptual difficulties.

435 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, Wellington, 2010) 58, R18.

If these functions are not to be carried out by the Privacy Commissioner, what other agency would fulfil them? Is it desirable for citizens to have a public official keeping an eye on privacy risks generally?

Q83 Do you have any concerns about the breadth of the Commissioner's functions? Should the functions be confined to matters involving informational privacy?

SHOULD ANY FUNCTIONS BE REMOVED OR CONSOLIDATED?

Consolidating the expression of the Commissioner's functions

6.51 Dealing with section 13 first, the Law Commission is struck by how long the list of functions is. Many of them overlap with others and some of them have not been exercised. It is the clear view of the Commission that the functions can be and should be formulated in a more succinct way. The current list is excessively long.

6.52 The issue was considered by the Privacy Commissioner in the first of the periodic reviews of the Privacy Act. There were some submissions that the list of functions is too long. However, the Commissioner felt that the functions should not be consolidated into a briefer list as each function fulfils an important purpose. He argued that the current formulation of the Commissioner's functions achieves a good balance between providing sufficient statutory authority for the Commissioner to act in a wide range of circumstances and specifying the Commissioner's functions in enough detail to ensure the Commissioner does not exceed his or her appropriate statutory remit.[436]

6.53 We agree that many of the current functions do serve important purposes. However, there is quite significant overlap between them, which could be removed. In our view, the list of functions in section 13 could be drafted more concisely without losing any of the value, by consolidating or amalgamating some of the functions.

Q84 We suggest that the Privacy Act should express the Commissioner's functions in a more succinct way. Do you agree? How could this best be done?

Removal of functions

6.54 In addition to expressing the Commissioner's functions more concisely, we believe that there are several functions that could be deleted, either because they are not necessary, or because they are not desirable for other reasons. We set out these functions below, with our reasons for suggesting that they be deleted.

436 *Necessary and Desirable* para 3.3.1.

Sections 13(1)(d) and 21 – directories of personal information

6.55 The origin of the function of maintaining and publishing directories of personal information was Principle 6 of the Privacy of Information Bill, which required each agency to maintain a document setting out the matters specified in sections 21(1)(a)-(f), along with a description of the information matching programmes in which the agency was involved. This principle was originally included to comply with the OECD Openness principle. The Openness principle's purpose is to encourage transparency about agencies' general practices for handling personal information. It states that:[437]

> 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.

However, its inclusion in New Zealand legislation was widely criticised, so the proposed Principle 6 was removed.[438] Section 21 is the last surviving trace of it in the current Act.

6.56 Section 21 is modelled on section 20 of the OIA, which requires the production of a periodic publication setting out the functions of departments and central government agencies. The objective appears to have been to assist members of the public to obtain personal information and therefore more effectively exercise their rights under the Act.[439] However, the Office has found that exercising this function presents significant practical difficulties, including resource constraints on the Office and likely compliance costs for agencies in supplying information if it were to be used. Therefore it has not been used.

6.57 This function was considered by the Commissioner in the first periodic review of the Act. The Commissioner then thought that there was no realistic possibility that a directory would ever be published, given resource constraints and the low priority of this work compared to the rest of the work of the Office. Furthermore, the Commissioner felt that in countries he had observed where directories were produced, they required a lot of resources and did not produce a significant public benefit. Therefore, he recommended that consideration be given to repealing sections 13(1)(d) and 21.[440]

6.58 However, he saw some value in directories in relation to the public sector, as they could assist individuals to exercise their rights and promote transparency and accountability. He therefore recommended that consideration be given to including some of the information listed in section 21(1) in the Directory of Official Information published by the Ministry of Justice.[441] He felt that this would be more efficient than producing a stand-alone directory.

---

437 Organisation for Economic Cooperation and Development *OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*, para 12.

438 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, 2007) PVA 21.3.

439 Privacy Act 1993, s 21(3).

440 *Necessary and Desirable* para 3.11, recommendation 40.

441 *Necessary and Desirable* para 3.11, recommendation 41.

6.59 Another possibility might be to impose a responsibility for openness falling directly on agencies themselves, or some class or classes of agency.

6.60 We discuss a potential new Openness principle in chapter 4.

Q85 We propose that sections 13(1)(d) and 21 should be deleted. Do you agree?

Sections 13(1)(c), (p), (q) and (r) – reports to the Prime Minister

6.61 These powers – to report to the Prime Minister on the monitoring of unique identifiers, on any matter affecting the privacy of individuals, on the desirability of the acceptance by New Zealand of any international instrument relating to the privacy of the individual, and on any other matter relating to privacy – have not been exercised.[442]

6.62 The Law Commission wonders whether these reports to the Prime Minister are necessary. It may be that some of the reporting functions are not necessary at all. But if it is decided to retain them, there is a question of who the various reports should be made to. There is no particular reason why these matters are of such importance that they should be dealt with by the Prime Minister rather than the line Minister who is responsible for the Privacy Act. If the issue is of such importance the Prime Minister will naturally become involved in it through the Cabinet process. Certainly, the Privacy Commissioner should have the function of reporting on matters that come within the range of her statutory remit, but we wonder whether there is any particular reason for reporting to the Prime Minister.

Q86 Are the reporting functions in section 13(1)(c), (p), (q) and (r) necessary? If so, is it necessary that the reports be to the Prime Minister?

Q87 Should any other functions in section 13 be removed?

SHOULD ANY FUNCTIONS BE AMENDED?

Section 26 – review of the operation of the Act

6.63 Section 26 requires the Commissioner to review the operation of the Privacy Act every five years. We believe that there is a serious question about whether it is appropriate for the Act to be reviewed by the Commissioner. It seems preferable that this task should be performed by an independent third party: that is, one that is independent from the executive government and has no stake in the outcome of the review. This independence is important because it helps ensure that a review is impartial and not influenced by considerations such as resources. This contributes to public confidence in the review process.

442 Note that there is also a power in section 81 to report to the Prime Minister in relation to an intelligence organisation.

6.64 The Privacy Commissioner might be thought to have a vested interest in the outcome of any review of the Privacy Act, as it directly affects his or her role and the operation of the Act that he or she is responsible for overseeing. While these perceptions may be unfair, they could detrimentally affect public confidence in the review, and consequently in the legislation itself. At the time of the first periodic review of the Act, there was in fact criticism that the Commissioner was not impartial because he had a strong ideological commitment to the privacy principles, and that therefore the public could not have confidence in the review process.[443]

6.65 Individuals and organisations who deal with the OPC may also be more frank in sharing their concerns about the operation of the Act with an independent reviewer rather than with the OPC, particularly if they had negative feedback about the Office. We think that perspective in any review would be valuable.

6.66 On the other hand, it might be said the Commissioner has significant expertise in the operation of the Act, and could therefore be in the best position to review it.

6.67 There is then a question of who ought to review the Act if not the Commissioner. Some possibilities might be the Ombudsmen, the Law Commission, the Ministry of Justice or a Parliamentary Select Committee. The Minister could also appoint an individual or form a special committee of experts.

6.68 Whether the Act still needs to be reviewed every five years is a further question. A longer review period such as ten years could be considered, or it may be thought that reviews are no longer required at all.[444] The Privacy Act is now well known, and seems to be relatively well accepted. Five-yearly reviews are resource-intensive, and there are not many other statutes that contain a similar requirement that they be reviewed periodically. The Evidence Act 2006 is one example.[445] There are also examples of such review provisions in privacy legislation in other jurisdictions.[446]

6.69 In our view, periodic reviews of all statutes are desirable. Reviewing legislation has a number of benefits including assessing how well legislation is working in practice, contributing to better regulation and improving implementation of the legislation.[447] So we think that this provision should be retained but that the review should be carried out by a person or organisation, other than the Privacy Commissioner, designated by the Minister.

443 *Necessary and Desirable* paras 3.16.3–3.16.9.

444 It is worth noting that the Health and Disability Commissioner has recently recommended that the requirement that he review the Health and Disability Commissioner Act 1994 every three to five years be changed to every ten years. The Commissioner felt that such frequent reviews are resource-intensive, time-consuming and often produce little change: Health and Disability Commissioner *A Review of the Heath and Disability Commissioner Act 1994 and Code of Health and Disability Services Consumers' Rights* (Wellington, 2009) 8–9.

445 Evidence Act 2006, s 202.

446 *Necessary and Desirable* para 3.16.2.

447 Law Commission (UK) *Post-Legislative Scrutiny* (The Stationery Office, London, 2006) 7–10.

6.70 Given the interrelationship between the Privacy Act and other acts such as the Official Information Act 1982, Local Government Official Information and Meetings Act 1987 and Public Records Act 2005,[448] consideration could also be given to conducting reviews of these Acts at the same time, so that consistency between them can be taken into account.

6.71 Finally, we think that there should be a requirement for the government to respond to reports arising out of these reviews within a specified period of time, such as six months.[449] The Commissioner has previously noted difficulties in implementing recommendations arising out of the first periodic review of the Act. It is now more than 10 years since the first review and there has been little legislative action. This has made it difficult to begin further five-yearly reviews of the Act as required. Furthermore, it is not clear what the government's view is of the recommendations, which creates difficulties for further reviews. The Commissioner therefore has recommended that a government response be required to be tabled in Parliament within six months. The next periodic review should be required five years from when the government response is received. This requirement could be introduced through amending section 26 or through Cabinet requirements or standing orders.[450] We agree that such a requirement would be useful.

Q88 We propose that a person or body other than the Privacy Commissioner should review the operation of the Act. Do you agree? If so, do you have any suggestions about who should conduct the reviews?

Q89 Should reviews continue to be required every five years?

Q90 We propose that there should be a requirement for the government to respond to reports arising out of reviews of the Act within a specified period of time. Do you agree?

Section 13(1)(b) – audits of personal information

6.72 Section 13(1)(b) currently allows the Commissioner, upon request of an agency, to conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether or not the information is maintained according to the privacy principles. No agency has asked to be audited, so no audits have been conducted.

6.73 Auditing has been used to promote compliance with the Privacy Act in two specific areas: information matching and credit reporting. In information matching, internal audits, whereby agencies audit themselves, are used as part

448 See chapter 11 for discussion of the interaction of the Privacy Act with these other statutes.

449 A similar requirement exists for Law Commission reports: Cabinet Office circular "Law Commission: Processes for Setting the Work Programme and Government Response to Reports" (24 April 2009) CO (09) 1, paras 20–24.

450 4th *Supplement to Necessary and Desirable* recommendation 46A.

of the process of granting authorisation and annual review.[451] Similarly, the Credit Reporting Privacy Code 2004 requires credit reporters to have internal audit programmes for data quality requirements and access controls.[452] Agencies that wish to access credit reporters' databases must agree to be audited by the credit reporter in relation to the provisions of the Code.

6.74 The Privacy Commissioner has recommended that she should have mandatory audit powers in relation at least to the public sector, but preferably to both public and private sectors.[453]

6.75 As we discuss further below, the Law Commission sees value in audits. Therefore, we think that the current audit power should be replaced with a more effective power. We now turn to discuss in more detail how such a power should be formulated.

Models of Audit

6.76 The term audit connotes a systematic assessment of an agency's compliance with the Privacy Act: that is, whether personal information is maintained in accordance with the privacy principles or relevant codes of practice, and any other relevant requirements of the Act, such as information matching rules. Within this broad description, there are several different ways in which an audit power could function. These include:

- a proactive overview to establish general compliance, resulting in a report and/or recommendations;
- an investigation into a specific area of suspected breach of the Act (this could also be characterised as investigation or enforcement action); or
- a requirement on agencies to regularly self-audit and report the results, perhaps in their annual reports, or in a separate report to the Privacy Commissioner.

Overseas Models

Canada

6.77 The Privacy Commissioner of Canada has the power to conduct audits of both public and private sector organisations. PIPEDA, which applies to the private sector, provides that the Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organisation if the Commissioner has reasonable grounds to believe that the organisation is contravening the Act. For the purpose of conducting audits, the Commissioner has the power to summon and enforce the appearance of people; to compel them to give evidence on oath and to produce records; to administer oaths; to receive and accept any evidence; and to enter premises

451 See further Office of the Privacy Commissioner *Information Matching Compliance Auditing Information Pack* (Wellington, 2008).

452 Credit Reporting Privacy Code 2004, rr 5, 8, 11 and sch 3.

453 4th *Supplement to Necessary and Desirable* para 2.11, Recommendation 37B.

occupied by the organisation and examine or obtain copies of records in the premises.[454] After an audit, the organisation is provided with a report containing the Commissioner's findings and any recommendations.[455]

6.78 The Privacy Act, which applies to the public sector, also provides that the Privacy Commissioner may carry out investigations to ensure compliance with the Act. Again, a report is provided containing the Commissioner's findings and recommendations.[456]

6.79 A number of provincial Privacy Commissioners also have audit powers, although some only have these powers in relation to the public sector.[457]

Australia

6.80 The Australian Privacy Commissioner has the power to conduct audits of records of personal information maintained by agencies (public sector organisations) for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles.[458] The Commissioner also has certain limited audit functions in relation to credit reporting and tax file numbers in the private sector. The Commissioner may audit a private sector organisation upon request by the organisation. Due to resource constraints, the Commissioner mainly conducts audits only when given specific funding to do so.[459]

6.81 The ALRC has recommended that the Commissioner's audit power be extended to cover the private sector. Audits would be called Privacy Performance Assessments, to emphasise their educational and non-confrontational focus.[460] The Australian Government, in its First Stage Response to the ALRC's report, has accepted this recommendation.

United Kingdom

6.82 Until recently, as in New Zealand, the UK Information Commissioner only had the power to conduct audits with consent. However, following high-profile data breaches, the Government proposed granting to the Commissioner power to conduct "spot-checks" on central government departments.[461] Section 173 of the Coroners and Justice Act 2009 has amended the Data Protection Act 1998 by

454 Personal Information Protection and Electronic Documents Act SC 2000, c 5, s 18(1).

455 Personal Information Protection and Electronic Documents Act SC 2000, c 5, s 19.

456 Privacy Act RSC 1985, c P-21, s 37.

457 See, eg, Freedom of Information and Protection of Privacy Act RSBC 1996 c 165, ss 42(1)(a) and 44 (British Columbia public sector); Personal Information Protection Act SBC 2003 c 63, s 36(1)(a) (British Columbia private sector); Freedom of Information and Protection of Privacy Act RSA 2000 c F-25, s 53(1) (Alberta public sector); Freedom of Information and Protection of Privacy Act CCSM c F175, s 49 (Manitoba public sector); An Act respecting access to documents held by public bodies and the protection of personal information RSQ c A-2.1, s 123 (Québec); An Act respecting the protection of personal information in the private sector RSQ c P-39.1, s 81 (Québec).

458 Privacy Act 1988 (Cth), s 27(1)(h).

459 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1581.

460 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1585–1588, R47-6.

461 Cabinet Office *Data Handling Procedures in Government: Final Report* (London, 2008).

conferring power on the Commissioner to issue an "assessment notice" on a government department or other designated agency for the purpose of determining whether it is complying with the data protection principles. The Commissioner is to issue a code of practice detailing how the function is to be exercised.[462]

Europe

6.83 Data Protection Commissioners in many European countries have audit powers. For example, the Spanish Data Protection Commissioner has the power to conduct systematic audits of the public and private sectors, as well as investigations into specific suspected breaches. Audits result in recommendations and a resolution, which can be appealed in court.[463]

Hong Kong

6.84 The Hong Kong Commissioner may carry out an inspection of personal data systems for the purpose of ascertaining information to assist the Commissioner to make recommendations.[464]

Discussion

6.85 Conducting privacy audits could have a number of advantages. Audits:

- would allow the Commissioner to be more pro-active in promoting compliance with the Act, rather than having to wait to receive a complaint;
- are likely to be more effective in uncovering systemic problems and promoting systemic improvement than the existing complaints system;
- could improve general compliance with the Act by providing an incentive for agencies to maintain compliance;
- could be used as an educative tool to improve privacy practices;
- could raise awareness of privacy among agencies and their staff; and
- would be likely to promote public confidence in New Zealand's information privacy protection regime.

6.86 The main potential disadvantage seems to be cost. The Office of the Privacy Commissioner would presumably require a significant increase in resources to be able to carry out audits in addition to the Commissioner's current functions. Overseas experience indicates that a lack of resources has often prevented Privacy Commissioners from fully exercising their audit powers. Audits would also impose costs on the agencies audited. There is, therefore, a risk that the burdens associated with audits could have a negative impact on perceptions of the Privacy Act. In the current environment, increased compliance costs are unlikely to be viewed favourably. Conversely, however, it is in agencies' interest to manage the personal information that they hold well. The costs of conducting

462 Coroners and Justice Act 2009 (UK), s 173, inserts new ss 41A-41C into the Data Protection Act 1998 (UK). Section 41C, which requires the Information Commissioner to produce a code of practice, came into force on 1 February 2010. Sections 41A and 41B will come into force at a later date.

463 Dr Artemi Rallo Lombarte "Auditing for Privacy Workshop: Chairman's Remarks" (Presentation to 2007 International Data Protection and Privacy Commissioners' Conference, Montréal, 26 September 2007).

464 Personal Data (Privacy) Ordinance, s 36.

audits must also be weighed against the costs of non-compliance with the Act (for example, economic losses for businesses who lose customers' loyalty due to poor privacy practices, or the resources required for the Privacy Commissioner to handle complaints).

6.87 Our provisional view is that, given the benefits associated with audits, the Privacy Act should provide for compulsory audits. However, the audit power should be developed so that it does not place an undue burden on agencies. We envisage that this power would provide a tool for the Privacy Commissioner to use if needed, and that the possibility of audits would help to encourage compliance generally; however, a comparatively small number of audits would be conducted.

6.88 What, then, should be the scope of the audit power? There are several options that could be explored. One option, as noted above, would be to require agencies to assess their own compliance. They could be required to publish reports detailing the personal information they hold and their compliance with the Privacy Act. This could have the advantage of giving agencies a sense of ownership of the audit process. The disadvantage, however, is that it places the full burden of an audit on the agency. The Privacy Commissioner would also probably have more expertise, so could conduct audits more easily than agencies could themselves. Self-audits could, however, sit alongside Commissioner audits and could be a useful tool for those agencies that wish to establish a reputation for following best practice.

6.89 Other options rely on the Privacy Commissioner to conduct audits. One approach, as in Canada, is to require that the Privacy Commissioner have reasonable grounds to believe that an agency is breaching the Privacy Act before the Commissioner may audit the agency. This approach has the advantage of being more limited in scope. Agencies that seemed to be complying would be left alone. However, this approach does not really allow the Privacy Commissioner to be proactive and to systematically examine the extent of Privacy Act compliance generally, which is one of the key benefits associated with audits. Conducting reactive audits upon finding some evidence of breaches of the Act within an agency (for example, through a complaint) may not be much of an advance on reacting to complaints. Having the power to proactively audit agencies would also allow the Privacy Commissioner to plan an audit programme with some certainty.

6.90 A further issue is whether the power to audit should extend to both the public and private sectors. In principle, we think that it should. Creating a separate regime for public and private sector agencies would be inconsistent with the principle that the Privacy Act applies equally to the public and private sectors. Furthermore, private sector agencies hold large amounts of personal information, and the Privacy Commissioner's public opinion surveys have shown that people are concerned about businesses breaching their privacy. Both public and private sectors are already used to audits in other areas. However, there are arguments for restricting audits to the public sector. Principles of government openness and accountability could suggest that there is a stronger public interest in allowing audits of the public sector than of the private sector. Given that one aspect of

public sector information management – recordkeeping – is already audited under the Public Records Act 2005,[465] Privacy Act audits could be seen as a logical next step.

6.91 Another question is how audits would be triggered. Given the potentially very wide extent of auditing, if the private sector is included and no suspicion of breach is required, some limitations would be needed. One natural limit will arise from the size and resources of the Commissioner's office – the Commissioner could only expect to audit a small number of agencies each year. While we think that it would be best not to require some suspicion that an agency is breaching the Act, audits could target areas of potential risk: for example, agencies that process large amounts of very sensitive personal information. The current Commissioner has previously indicated that she would prioritise audits in areas such as the public sector, credit reporting and health information systems.[466] Consideration could also be given to exempting certain agencies such as small businesses from audit requirements, given the large burden that an audit would place on a small business. However, some small businesses such as small internet service providers might hold significant amounts of personal information. A better approach might be for the Commissioner to have discretion to take into account factors such as the size of agencies and the kinds of information they hold in deciding which agencies to audit.

6.92 The powers associated with audits would also need consideration. Overseas experience indicates that audits are best used as a tool to educate agencies and encourage compliance, rather than as a punitive tool. Normally the Commissioner would report and make recommendations. Consideration could be given, in appropriate cases, to making the report public. This would of course not prevent the Commissioner from exercising his or her general powers. For example, if the Commissioner is given the power to issue enforcement notices (as discussed in chapter 8), he or she could issue an enforcement notice if a problem was discovered during an audit. While the Commissioner would not have additional punitive powers specifically associated with audits, he or she would need sufficient powers to be able to carry out the audit effectively if there was some resistance from the agency. These would include the power to enter an agency's premises and to examine or obtain copies of records.

Proposal

6.93 Our tentative proposal is that the Privacy Commissioner be given mandatory audit powers. Features of the audit power would be that:

- it would cover public and private sectors;
- it would be proactive (that is, it would not be contingent upon suspecting a breach of the Act);
- the Commissioner would have to give reasonable notice of his or her intention to audit an agency; and
- the Commissioner would report his or her findings and recommendations to the agency, but would not have further coercive powers particular to audits.

---

465 Public Records Act 2005, s 33. Audits are due to begin in 2010, and agencies will be audited every five to ten years.

466 4th *Supplement to Necessary and Desirable* para 2.11.

The Commissioner would, however, be able to use any general powers available to him or her.

Q91 We propose that the current audit power should be amended to give the Commissioner power to conduct mandatory audits, as outlined in paragraph 6.93. Do you agree?

Q92 Should any other functions be amended?

ARE ANY ADDITIONAL FUNCTIONS OR POWERS REQUIRED?

6.94 In chapter 8 we outline our proposal that the Commissioner should be able to issue enforcement notices. We do not repeat this discussion here, but note that this proposal would entail some additions to the Commissioner's existing functions and powers.

6.95 In our view, the Commissioner's ability to monitor and promote compliance with the Act will be significantly enhanced by the ability to conduct mandatory audits, as well as other reforms discussed in this paper, such as the ability to issue enforcement notices. We also recommended in our report on stage 3 of this Review that the Commissioner should have a new function of reporting on developments in surveillance or surveillance technologies.[467] We also ask in chapter 13 of this issues paper whether the Commissioner should have further powers to monitor and report on developing technology in general. Apart from this, we do not think that further powers are required. However, we are interested in receiving submissions on this point.

Q93 Do you think that the Commissioner should have any further functions or powers that we have not discussed?

467 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, Wellington, 2010) Recommendation 18.

Chapter 7
Codes of practice

7.1 This chapter covers the issuing of codes of practice under Part 6 of the Privacy Act. As discussed in chapter 2, the open-textured, principles-based approach of the Act means that agencies have a great deal of flexibility when it comes to determining how they will comply with the Act. Codes of practice supplement this flexibility by providing a mechanism through which the specific needs and circumstances of particular agencies, businesses, industries, or professions can be accommodated.

7.2 In this chapter, we cover:

- the existing framework for issuing codes of practice;
- an overview of the current codes;
- a comparison of the Australian and United Kingdom approaches; and
- some possible changes to the Act.

7.3 Under section 63 of the Act, the Privacy Commissioner can issue codes of practice in relation to public registers.[468] Stage 2 of our Review looked at the law relating to public registers.[469] The public register provisions of the Act are therefore outside the scope of this issues paper.

7.4 In considering the code-making framework, we do not wish to question the merit or otherwise of any particular code. Specific codes are outside the scope of the review, and we seek comments only in relation to the code-making framework, not the content of any particular code.

468 The power has never been exercised. Note, however, that the Credit Reporting Privacy Code 2004, cl 4(2)(b), states that the Code modifies the application of public register privacy principle 2. In addition, authority to issue codes of practice in relation to public registers is conferred on the Privacy Commissioner by sections 122 and 123 of the Domestic Violence Act 1995.

469 New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008). The recommendations in this report will be considered by the Government once the Law Commission finishes its review of the Privacy Act. They will be drawn together in our final report.

THE EXISTING FRAMEWORK

7.5 Part 6 of the Act empowers the Privacy Commissioner to issue codes of practice.[470] A code of practice may apply in relation to information of certain kinds, or in respect of certain kinds of agency, activity, industry, profession, or calling.[471] A code of practice may:[472]

- modify the application of any one or more of the privacy principles by prescribing standards that are more or less stringent than a principle, or exempt any action from a principle unconditionally or subject to conditions;
- apply any one or more of the privacy principles (but not all of them) without modification;
- prescribe how any one or more of the privacy principles are to be applied or complied with;
- impose controls on information matching carried out by agencies that are not public sector agencies;
- set guidelines to be followed by agencies in determining charges under section 35, and prescribe circumstances in which a charge may not be imposed;
- prescribe procedures for dealing with complaints of breaches of a code (so long as the code provisions do not limit or revise the provisions in Parts 8 and 9 of the Act); and
- provide for the review of a code and for its expiry.

7.6 By prescribing standards that are more stringent than the standards prescribed by any one or more of the privacy principles, codes of practice can provide enhanced privacy protection. In this way, codes can regulate an area that would otherwise be unregulated. The Credit Reporting Privacy Code 2004, through the limitations that it places on the kinds of personal information that credit reporters can collect, is a good example of this. Conversely, the codes can provide for less stringent requirements than those required by the Privacy Act, thereby effectively exempting agencies or certain sectors from the Act's or the privacy principles' requirements.

7.7 The power to issue codes of practice is therefore very wide, but there are limits on what a code of practice could do. For example, a code could not extend the ambit of the Act to agencies to which it does not currently apply, or override or modify other enactments. In addition, a code cannot limit or restrict the rights conferred on individuals by principle 6 and principle 7 to access and correct personal information held by public sector agencies.[473]

7.8 Section 53 of the Act sets out the effect of a code. For the purposes of the complaints procedures in Part 8 of the Act, doing something that would ordinarily be a breach of a privacy principle is not a breach if it is done in compliance with a code, and failing to comply with a code is a breach of a privacy principle, even though it would not ordinarily be a breach of such a principle.[474]

470 Privacy Act 1993, Part 6.

471 Privacy Act 1993, s 46(3).

472 Privacy Act 1993, s 46.

473 Privacy Act 1993, s 46(5).

474 Privacy Act 1993, ss 53(a) and (b).

7.9 The Privacy Commissioner can issue a code of practice on his or her own initiative, or on application by someone else.[475] There are limitations on who can submit a proposed code to the Commissioner for approval and issue.[476] The applicant must be a body whose purpose, or one of whose purposes, is to represent the interests of any class or classes of agency, or of any industry, profession, or calling. The proposed code must be intended to apply either in respect of those whom the applicant represents or in respect of an activity that they undertake.

7.10 The Act prescribes the procedure that must be followed before a code can be issued. At a minimum, the Commissioner must give public notice of the intention to issue a code, the details of the proposed code, and information about where copies of a draft of the proposed code can be obtained, and must invite submissions on the proposed code.[477] The Commissioner is required to do everything reasonably possible on his or her part to advise people who will be affected by the proposed code, or their representatives, of the terms of the proposed code, and of the reasons for it.[478] The Commissioner must also give those persons or their representatives a reasonable opportunity to consider the proposed code, and make submissions on it, and must also consider those submissions. These procedures also apply with respect to the amendment or revocation of a code.[479]

7.11 The code of practice development process is therefore lengthy and relatively complex. The consultation requirements are a significant part of the process.[480] One commentator has observed that a side benefit of the process is that "agencies requesting the codes are well-versed in their privacy obligations and responsibilities by the time the applicable standard has been reflected within their code".[481]

7.12 A notice must be published in the *Gazette* notifying the issuing of a code of practice, and where copies can be inspected and purchased, and the Commissioner must ensure that copies of a code are available for public inspection free of charge, and for purchase at a reasonable price, while the code remains in force.[482] A code cannot come into force earlier than the 28th day after its notification in the *Gazette*.[483]

---

475 Privacy Act 1993, s 47(1).

476 Privacy Act 1993, s 47(3).

477 Privacy Act 1993, s 48(a).

478 Privacy Act 1993, s 48(b).

479 Privacy Act 1993, s 51(2).

480 The Privacy Commissioner has issued a Guidance Note about codes and the process by which they are made: *Guidance Note on Codes of Practice Under Part VI of the Privacy Act* (Wellington, 1994). The note highlights, in particular, the importance of consultation in the development of codes, not just with industry or professional groups to which the code would apply but also with people about whom information is held.

481 Elizabeth Longworth "Developing Industry Codes of Practice and Policies for the Australian Private Sector" [1996] PLPR 12.

482 Privacy Act 1993, s 49(1).

483 Privacy Act 1993, s 49(2).

7.13 Provision is made for the urgent issuing, amendment, or revocation of a code without following the ordinary consultation procedures.[484] Under section 52 of the Act, the Privacy Commissioner can do this if he or she considers that it is necessary to issue, amend, or revoke a code urgently and that for that reason it would be impracticable to follow the ordinary procedure. A code of practice, or an amendment or revocation of a code of practice, issued under section 52 cannot remain in force for longer than one year.[485]

7.14 Codes of practice are a form of delegated legislation known as "deemed regulations".[486] They are issued by the Commissioner rather than by the Parliamentary Counsel Office and do not go through the normal Cabinet approval process that applies to ordinary statutory regulations. The Acts and Regulations Publication Act 1989 does not apply to them, and they are not published in the Statutory Regulations series.[487] However, codes must be presented to the House of Representatives after they are made, and are subject to disallowance under the Regulations (Disallowance) Act 1989.[488]

CURRENT CODES

7.15 There are three main codes of practice currently in force:

- Health Information Privacy Code 1994;
- Telecommunications Information Privacy Code 2003; and
- Credit Reporting Privacy Code 2004.

We explain each of these in turn below.

7.16 In addition, there are two codes of practice that relate to unique identifiers, and modify the application of principle 12 in particular circumstances to allow unique identifiers assigned by one agency to be used by another. These are as follows:

- Superannuation Schemes Unique Identifier Code 1995; and
- Justice Sector Unique Identifier Code 1998.

7.17 To date, three codes have been revoked or have expired.

Health Information Privacy Code 1994

7.18 The Health Information Privacy Code (HIPC) has the broadest application. It applies to "health information" held by a "health agency", both terms being very widely defined. A code relating to health information was first issued as a temporary code in July 1993, and was replaced by a permanent code in 1994.[489] The code essentially substitutes a set of 12 rules relating to health information in place of the privacy principles. In some cases, the rules substantially repeat

484 Privacy Act 1993, s 52.

485 Privacy Act 1993, s 52(2).

486 Privacy Act 1993, s 50. For further information on deemed regulations, see "What are Deemed Regulations?" on the Parliamentary Counsel Office website at www.pco.parliament.govt.nz/what-are-deemed-regulations.

487 Privacy Act 1993, s 50.

488 Privacy Act 1993, s 50.

489 The latest edition of the code was published in December 2008, and incorporates Amendment Nos 1-6. Available online at www.privacy.org.nz/health-information-privacy-code.

the provisions of the privacy principles. In others, the privacy principles are modified by adding additional requirements or omitting requirements in a principle that are not relevant in a health context.

7.19 The most significant modifications are made in relation to principle 11 (limits on disclosure of personal information), of which rule 11 of the HIPC is the equivalent. Rule 11 supplements the general circumstances set out in principle 11 in which information can be disclosed without the consent of the individual by recognising and codifying what has been described as the "many long-established disclosure practices of the health professions".[490] An example is information in general terms about the presence, location, condition, and progress of a patient in a hospital, unless disclosure would be contrary to the express request of the patient or his or her representative.

7.20 It should also be noted that, although the Act does not usually apply to personal information about deceased persons, section 46(6) of the Act provides that any code of practice relating to health information is to have effect as though principle 11 applied to information about both living and deceased persons. Rule 11 of the HIPC states that it applies to health information about both living and deceased persons, but excludes information about persons who have been dead for 20 years or more.

7.21 The complexity of this area of the law is possibly a good justification for having a specific code about health information. The complexity can then, to the extent possible within the limits of a code of practice, be accommodated in a more useful and helpful way than simply relying on the more general privacy principles. The format of a code issued by OPC can also be helpful. The versions of the HIPC issued by the Privacy Commissioner contain a commentary, along with background and explanatory material and practical examples to illustrate the application of the code. These have also been supplemented by other OPC publications such as *On the Record: A Practical Guide to Health Information Privacy*, the second edition of which was issued in July 2000.[491]

7.22 A 2002 review by the Mental Health Commission of the way in which District Health Board mental health services are interpreting the Privacy Act and the HIPC found that there is confusion and misunderstanding amongst clinicians about the requirements of the Act and the Code, and their relationship with other key pieces of legislation, such as the Mental Health (Compulsory Assessment and Treatment) Act 1992 and some provisions of the Health Act 1956. Importantly, however, the review concluded that legislative change was not required to address the issues identified.[492] The current legislation was considered to provide a framework which enabled practitioners to make sound decisions on sharing information. What was required was better understanding by staff of the existing legislation pertaining to information-sharing, and clearer

490 PDG Skegg and Ron Paterson (eds) *Medical Law in New Zealand* (Thomson Brookers, Wellington, 2006) 299.

491 Office of the Privacy Commissioner *On the Record: A Practical Guide to Health Information Privacy* (2 ed, Wellington, 2000).

492 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* (Wellington, February 2002) 10.

information-sharing policies and practices, specific to mental health services. There also needed to be better communication of the current rules and policies, and compliance with both by mental health services staff.

7.23 Of the three main codes of practice, the HIPC generates the highest number of complaints. In the 2008–09 year, the Office of the Privacy Commissioner (OPC) received 147 complaints relating to the three principal codes, of which 139 related to the HIPC.[493] This no doubt reflects the broader scope of the HIPC compared with the other two codes of practice. Of the 81 privacy cases that were brought before the Human Rights Review Tribunal between 1993 and 2006, 12 cases (15 per cent) were brought under the HIPC.[494] The highest award of damages to date for a Privacy Act complaint, $40,000, was made in a case involving the disclosure of health information.[495]

7.24 While it appears that the HIPC is generally operating well, experience with the HIPC also illustrates the limitations of a code of practice in an area of law as complex as health information. The code must also coexist and interrelate with a complex web of other health-related legislation, such as sections 22B to 22H of the Heath Act 1956, and the Code of Health and Disability Services Consumers' Rights issued under the Health and Disability Commissioner Act 1994, as well as health practitioners' ethical duties and long-standing industry practices.[496] While we include no final view in this paper, we ask in chapter 19 whether health information may need its own, separate legal regime.

Telecommunications Information Privacy Code 2003

7.25 The Telecommunications Information Privacy Code (TIPC) was issued in 2003. The code has its origins in a draft code jointly prepared by a working group of the then principal network operators (Telecom, BellSouth, and Clear Communications). Those operators presented their draft code to the Privacy Commissioner in 1997, and asked the Privacy Commissioner to consider issuing their draft code under the Act.[497] Resourcing issues, coupled with the need for subsequent work by the Privacy Commissioner, prevented the then Privacy Commissioner from advancing the proposed code for some years, and a draft code was not released for public consultation until December 2001.

7.26 The TIPC applies to "telecommunications agencies" (which includes network operators, publishers of directories of subscribers of telecommunications services, internet service providers, and mobile telephone retailers) with respect to personal information about subscribers, information generated as a result of a

493 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 25.

494 Gehan Gunasekara and Erin Dillon "Data Protection Litigation in New Zealand: Processes and Outcomes" (2008) 39 VUWLR 457, 472.

495 *Hamilton v The Deanery 2000 Ltd* [2003] NZHRRT 28.

496 Some of the complexities of the relationship between the HIPC and section 22F of the Health Act 1956 are explored in Nicola S Peart "Access to, and Disclosure of, Health Information: Are the Rules in Need of a 'New Treatment'?" (1996) 2 HRLP 95. The Public Health Bill 2007, no 177-2, if enacted, would repeal and replace the Health Act 1956. The provision of the Bill that is equivalent to section 22F is clause 24. We discuss the interrelationship of the Privacy Act and the Health and Disability Commissioner Act in chapter 11.

497 See further Office of the Privacy Commissioner "Telecommunications Privacy Issues in New Zealand 1995–1998" [1998] PLPR 29.

telecommunication, and the content of a telecommunication. To the extent that it applies, the code effectively substitutes 12 telecommunications information privacy rules for the privacy principles, although some of the principles are applied without modification.

7.27 The TIPC deals with the inclusion and availability of the contact details of subscribers in or through directories and directory services, and the use of Calling Line Identification Presentation (commonly known as "caller ID"). Restrictions on the use of telecommunications for the purpose of direct marketing are also imposed. Specific provision is made for collection, use and disclosure "for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity."

7.28 The TIPC is reasonably complex, and relies on a number of definitions from other pieces of legislation, particularly the Telecommunications Act 2001. The code is also noteworthy in that it requires telecommunications agencies to set up and operate their own internal complaints-handling process, although this does not displace the right of persons to complain directly to the Privacy Commissioner.

7.29 The Regulations Review Committee (RRC) considered the TIPC in 2003/04 and raised concerns about two aspects of the code (as originally issued).[498] The Privacy Commissioner subsequently amended the TIPC to meet these concerns. The RRC was satisfied with the amendments.

7.30 Only one complaint relating to the TIPC was received by the Privacy Commissioner in the 2008/09 financial year.[499]

Credit Reporting Privacy Code 2004

7.31 Credit reporting companies hold vast amounts of information about people. Some of the information held by credit reporting companies is highly sensitive, and reflects on a person's financial reputation.[500] These companies collect masses of information every day. For example, Veda Advantage, which operates in both Australia and New Zealand, states that it collects data on more than 16.5 million individuals and 4.4 million companies in New Zealand and Australia, and each day generates credit reports on 60,000 individuals and businesses on both sides of the Tasman that apply for credit.[501]

7.32 The Credit Reporting Privacy Code (CRPC) was issued in 2004, and became fully operational in April 2006. It has been amended three times, once by a temporary amendment. As with the TIPC, resourcing issues in the OPC in the

498 Regulations Review Committee *Activities of the Regulations Review Committee in 2004* (April 2005).

499 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 25. Ten complaints were received in the previous year under the TIPC.

500 Further, most of the information about a person is collected from sources other than the person himself or herself. It has been provided by banks, utility companies such as telecommunications, electricity, and gas suppliers, and retailers, or it is sourced from publicly-available information, for example bankruptcy notices. The information is made available by credit reporting companies to a wide range of agencies, in most cases without the subject of the information knowing about it.

501 Veda Advantage "What We Do" www.vedaadvantage.com/about-veda/nz_about-what-we-do.dot (accessed 10 February 2010).

late 1990s stalled progress on the code, and a proposed code was not issued for public consultation until 2003. The Privacy Commissioner has noted that the credit industry was fully engaged during the statutory consultation process and in subsequent discussions, making many helpful suggestions about the workability of proposed solutions and ways to minimise compliance costs. As a result, substantial changes were made to accommodate these suggestions.[502]

7.33 The CRPC addresses key concerns about credit reporting by:[503]

- limiting the information that may be contained in credit reporting systems
- controlling who may have access to the information
- reducing opportunities for misuse
- enhancing the transparency and openness of the process
- ensuring that individuals are made aware of their rights and that disclosures are properly authorised
- establishing standards to avoid mismatching information about different individuals
- ensuring information is regularly updated
- requiring access logs to be maintained
- removing the financial barriers to "self-auditing" by requiring credit reporters to provide individuals on request with free copies of any credit information held about them
- providing greater certainty about how long information will be retained
- requiring disputed information to be flagged or suppressed while its accuracy is determined
- requiring prompt low-level dispute resolution.

7.34 A key aspect of the CRPC is the limitation it imposes on information that credit agencies can include in their systems. A credit reporter can only collect personal information for the purpose of credit reporting if the information falls within the definition of "credit information". The definition includes identifying information about the individual, information about an application for credit (such as the type of credit and the amount sought), credit default information (such as the date of default, the amount in default, and when the amount in default was finally settled), information about any summary instalment orders or judgments for monies owed against the individual, bankruptcy information (adjudications, discharges, suspensions, and annulments), and information sourced from certain public

502 Office of the Privacy Commissioner *General Information Paper on the Credit Reporting Privacy Code* (Wellington, December 2004).

503 Office of the Privacy Commissioner *Privacy Commissioner Annual Report for the year ended 30 June 2006* (Wellington, 2006) 26.

registers. The essential feature of this information is that it is negative in character.[504] It does not include information tending to establish a person's good credit history, such as timely repayment of loans without defaults.

7.35 A further feature of the CRPC is that it applies directly only to credit reporting agencies. Credit providers (such as banks and finance companies) and other agencies (subscribers) that obtain credit reports (such as debt collectors, prospective employers, prospective insurers, and prospective landlords) are covered indirectly, through the agreements with credit reporting agencies under which they access credit information. The privacy principles still apply to credit providers and other subscribers.

7.36 Compatibility with the way in which credit reporting is regulated in Australia is also a significant issue, given the close relationship between the New Zealand and Australian markets. The Australian Law Reform Commission (ALRC) has reviewed the credit reporting provisions in the Privacy Act 1988 (Cth) and made recommendations for changes to those provisions.[505]

7.37 The CRPC provides that the Privacy Commissioner must review the code as soon as practicable after 1 April 2008. A review of the CRPC is currently underway. As part of the review process, the Privacy Commissioner set up a reference group, consisting of a selection of key stakeholders (credit reporting agencies, credit providers, government agencies, privacy experts, and consumer groups).[506] One of the most contentious issues for consideration in the review of the CRPC is undoubtedly whether or not New Zealand should move from its current negative reporting regime to positive or more comprehensive credit reporting.

7.38 Seven complaints relating to the CRPC were received by the Privacy Commissioner in the 2008/09 financial year.[507]

---

504 "Negative" and "positive" are terms commonly used in relation to credit reporting. The Australian Law Reform Commission explains them as follows: "As the term suggests, negative credit reporting involves 'negative' information – that is, information that detracts from an individual's credit worthiness, such as the fact that he or she has defaulted on a loan. On the other hand, positive credit reporting is said to involve 'positive' information about an individual's credit position and includes information relating to that person's current credit commitments. An example of information in this category is a record of an individual having made a loan repayment." However, the ALRC goes on to caution that this distinction is something of an oversimplification and can be somewhat misleading. Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) 1800–1802.

505 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) chs 52–59. There are currently significant differences between Australian and New Zealand law with respect to whether a credit reporting agency in one jurisdiction can supply a credit report in response to a request made in the other jurisdiction. New Zealand law permits cross-jurisdictional requests for credit reports, but Australian law does not. The ALRC report recommends that the Australian restriction be relaxed in certain circumstances (see recommendation 54–7).

506 See Victoria Hinson, Lazar Associates Ltd *Review of Credit Reporting Privacy Code 2004: Report of Reference Group Discussions – June 2009* (Office of the Privacy Commissioner, Wellington, 2009). The New Zealand Law Commission was a member of the reference group as an independent observer.

507 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 25.

A COMPARISON OF OVERSEAS APPROACHES

7.39 In the following section we examine the approaches to privacy protection through codes of practice in Australia and the United Kingdom.[508]

Australia

Federal

7.40 The original Privacy Act 1988 (Cth) applied only to Federal government agencies, and made no provision for the issuing of codes of practice. The Act was extended to credit reporting agencies and credit providers in 1990, and the Privacy Commissioner was required to issue a code of conduct relating to credit reporting. The Australian Privacy Commissioner issued the Credit Reporting Code of Conduct in September 1991. Compliance with the Code of Conduct is mandatory for credit reporters and credit providers, and breaches constitute an interference with privacy for the purposes of the investigation and enforcement provisions of the Act.

7.41 The Privacy Act 1988 (Cth) was extended by the Privacy Amendment (Private Sector) Act 2000 to cover private sector organisations (which are referred to in the Act as "organisations", in contrast to public sector "agencies"). As part of that extension, organisations were provided with the option of developing their own privacy codes for the handling of personal information,[509] which, if approved by the Australian Federal Privacy Commissioner, take the place of the National Privacy Principles for the organisations subject to the code. Unlike in New Zealand, the Australian Privacy Commissioner cannot initiate a privacy code, and a code is not binding on organisations that do not consent to be bound by it. Codes will only be approved by the Privacy Commissioner if they provide at least as much privacy protection as the National Privacy Principles; thus, codes cannot provide for less stringent requirements than the Act requires. The approach was "designed to allow for flexibility in an organisation's approach to privacy, but at the same time, guarantees consumers that their personal information is subject to minimum standards that are enforceable in law."[510] The inclusion of the privacy code mechanism as part of the extension of the Act to the private sector reflected the government's view that co-regulation of the private sector with respect to privacy was preferred over self-regulation or full regulation.[511]

7.42 Commenting on the code provisions in the Australian Act, Nigel Waters observed:[512]

> It remains to be seen whether private sector organisations find it worthwhile to develop and submit codes for approval. Given that the standards cannot be less than the NPPs, the only advantage to an organization or industry sector in submitting their own principles would seem to be the opportunity to couch them in industry specific

508 Canadian privacy legislation does not make provision for the development of codes and thus is not considered here.

509 Privacy Act 1988 (Cth), Part IIIAA.

510 Office of the Privacy Commissioner (Cth) *Guidelines on Privacy Code Development* (Sydney, 2001) 16.

511 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 48.2.

512 Nigel Waters "Codewatch: Privacy Codes – What are They? Where are They?" [2001] PLPR 6.

language. In relation to complaint handling, some sectors may perceive an advantage in providing for privacy complaints to be handled in the first instance by an industry specific body (a code adjudicator under the Act), although this advantage was arguably eroded by a late amendment to make determinations of code adjudicators subject to appeal to the Commissioner — replacing a more limited but more powerful right to judicial review.

7.43 At the date of writing, there were only three approved codes listed on the website of the Office of the Australian Privacy Commissioner.[513]

7.44 In a review in 2005 of the operation of the private sector provisions of the Privacy Act, the Office of the Australian Privacy Commissioner made the following comments on the operation of codes under the Act:[514]

> Another area where the objectives of the private sector provisions have not been achieved in the way that was anticipated is the adoption of industry and organisation codes by the private sector to regulate their collection, use and disclosure of personal information. There are only three approved codes under the Privacy Act. However, there is no call for the repeal of the code provisions of the Act despite the very low level of take-up. Most businesses appear content to be regulated by the NPPs and to have the Office as their external complaints handling body.

7.45 Submissions to the Office of the Australian Privacy Commissioner as part of that review suggested that the development and approval process for codes was unduly long, onerous, complex, and costly. The Office accordingly recommended that it review the Code Development Guidelines dealing with the processes relating to code approval with a view to simplifying them.[515] The Office also recommended that the Privacy Commissioner be empowered to issue binding codes.[516]

7.46 As part of its review of the Privacy Act, the ALRC sought submissions on the question of codes.[517] The ALRC's report indicates that responses identified support for the existing co-regulation model in the Privacy Act, but also raised issues about the complexity of the privacy regime as a result of voluntary codes, and the resource-intensive nature of the code-making process, which was considered to have little identifiable benefit.[518]

---

513 These are the Market and Social Research Privacy Code, the Queensland Club Industry Privacy Code, and the Biometrics Institute Privacy Code. The website also indicates that one application for approval of a code is currently being considered by the Privacy Commissioner: the Internet Industry Privacy Code. See www.privacy.gov.au/business/codes/register (accessed 11 February 2010).

514 Office of the Privacy Commissioner (Cth) *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Sydney, 2005).

515 Office of the Privacy Commissioner (Cth) *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Sydney, 2005) recommendation 47.

516 Office of the Privacy Commissioner (Cth) *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy* Act 1988 (Sydney, 2005) 46–47.

517 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) ch 48.

518 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 48.10.

7.47 In its recommendations, the ALRC considered that privacy codes under the Privacy Act 1988 (Cth) should operate more like the way in which codes operate in New Zealand. Taking a set of recommended Unified Privacy Principles (UPPs) as the base standard, the ALRC recommended that privacy codes should operate in addition to the UPPs, rather than replacing the UPPs as is currently the case.[519] The Government response accepted this recommendation in principle, but noted that while a code cannot derogate from the UPPs, there was no reason why it should not expand upon or enhance them.[520] To that extent it might "replace" them.

7.48 The ALRC did not recommend that the Privacy Commissioner should have power to issue binding codes, despite strong support among stakeholders.[521] The Government response, however, supports a power for the Commissioner to *request* an organisation to develop a code; and then, if an adequate code is not developed, a power in the Commissioner himself or herself to develop and impose a mandatory code.[522] Breach of such a mandatory code would be an interference with privacy under the Act, and subject to enforcement mechanisms.[523]

New South Wales

7.49 Under the New South Wales Privacy and Personal Information Protection Act 1998, codes of practice may be initiated and developed by the NSW Privacy Commissioner or any public sector agency, and then submitted to the responsible Minister (currently the Attorney-General).[524] The responsible Minister can then decide whether or not to make the code.[525] Codes are drafted by the Parliamentary Counsel's Office, made by order of the responsible Minister, and published in the Gazette.[526] Codes can modify the application of one or more of the information protection principles as they apply to any particular public sector agency (the Act does not apply to the private sector) by:

- specifying requirements that are different from the requirements set out in the principles, or exempting any activity or conduct of or by the agency from compliance with any such principle;
- specifying the manner in which any one or more of the information protection principles are to be applied to, or are to be followed by, the agency; or
- exempting the agency, or any class of public sector agency, from the requirement to comply with any information protection principle.

---

519 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) recommendation 48 -1.

520 Australian Government *Enhancing National Privacy Protection. Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 89.

521 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 48.34.

522 Australian Government *Enhancing National Privacy Protection. Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 89–90.

523 Australian Government *Enhancing National Privacy Protection. Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 90.

524 Privacy and Personal Information Protection Act 1998 (NSW), Part 3.

525 Privacy and Personal Information Protection Act 1998 (NSW), s 31(4).

526 Privacy and Personal Information Protection Act 1998 (NSW), s 31(5).

7.50 Importantly, the Act states that codes may not impose requirements on public sector agencies that are more stringent (or of a higher standard) than those of the information protection principles.[527] Agencies to which any particular code applies must comply with its provisions.[528]

United Kingdom

7.51 The Data Protection Act 1998 is the United Kingdom's primary data protection law. An Information Commissioner oversees compliance with the Act. Codes of practice are recognised by the Act as follows:

- Section 51 of the Act imposes a duty on the Information Commissioner "to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers". If directed by the Secretary of State or if the Information Commissioner considers it appropriate to do so, the Commissioner is to prepare and disseminate appropriate codes of practice for guidance as to good practice. Appropriate consultation with trade associations, data subjects or persons representing data subjects must precede the issuing of a code of practice.
- Section 51(4) provides that the Commissioner must, where he or she considers it appropriate to do so, encourage trade associations to prepare and disseminate codes of practice to their members. The Commissioner must also consider any code of practice submitted to him or her by a trade association, and after such consultation with data subjects or persons representing data subjects as appears to the Commissioner to be appropriate, notify the trade association whether in the Commissioner's opinion the code promotes the following of good practice. The term "trade association" is defined as any body representing data controllers.

7.52 The Information Commissioner has issued a number of codes of practice under section 51(3).[529] An example of an industry-developed code of practice endorsed by the Information Commissioner under section 51(4) of the Act is the code of practice for archivists and records managers.

7.53 Codes of practice issued under section 51 do not have the same legal status as codes of practice issued under the New Zealand Privacy Act. A departure from a code is not unlawful, and the basic legal requirement remains compliance with the Data Protection Act itself. A code sets out the Information Commissioner's recommendations about how to meet the legal requirements of the Act, but data controllers may have alternative ways of meeting those requirements. Enforcement action against a data controller would still be based on a failure to meet the requirements of the Act, but the Commissioner is likely to refer to the Code and ask the data controller to justify any departure from the code.

527 Privacy and Personal Information Protection Act 1998 (NSW), s 29.

528 Privacy and Personal Information Protection Act 1998 (NSW), s 32.

529 Code of Practice on Telecommunications Directory Information Covering the Fair Processing of Personal Data (1998); Employment Practices Code (2005); CCTV Code of Practice (2008); Privacy Notices Code of Practice (2009). The Information Commissioner has also issued a Framework Code of Practice on for Sharing Personal Information (2007), which is designed to assist organisations to produce their own code of practice on information sharing.

Observations

7.54 By comparison with codes of practice in other jurisdictions we have examined, the New Zealand codes of practice are significantly more potent. Codes of practice in New Zealand can modify the privacy principles, can prescribe standards that are more stringent or less stringent, or can exempt actions from the privacy principles. Australian Federal codes cannot prescribe standards that are less than the National Privacy Principles. In New South Wales, codes cannot be more stringent, or impose higher standards on public agencies than the relevant privacy principles require. Codes of practice in New Zealand have legal status, something they do not have under the United Kingdom Data Protection Act 1998. In Australia, at the Federal level, codes are only binding by consent, although that may be about to change.

OPTIONS FOR REFORM

General views

7.55 Few codes of practice have been issued under the Privacy Act 1993 during the 17 years since the Act was passed. The Privacy Commissioner noted in *Necessary and Desirable* that when the Bill was being enacted it was expected that codes would be required for the banking and insurance industries, but none had been forthcoming.[530] This remains the case.

7.56 On this basis, our overall conclusion is that the principles-based approach in the Privacy Act, together with the guidance and advice provided by the OPC, is working satisfactorily for most agencies to which the Act applies, without the need for a code of practice.

7.57 This is not to diminish the importance of the code of practice mechanism in the Privacy Act. The codes that have been issued in New Zealand, while small in number, cover some key areas such as the health and telecommunications sectors. The value of a code-making provision as a "reserve power", to be used if other measures fail, should also not be underestimated. The practice of the current Privacy Commissioner is to try "light-handed" regulatory measures, such as guidelines, first, before escalating to a code of practice.

7.58 Subject to what we say below, our research has not uncovered significant problems with the code of practice mechanism in the Privacy Act. It appears to be working satisfactorily, a view shared by the OPC. The limitations, however, on what a code of practice can achieve in an area where privacy is only one part of a complex web of law and practice is apparent from the Health Information Privacy Code.

7.59 We consider that most aspects of the code-making process are necessary and desirable, and would not propose to change them. The Privacy Commissioner is an independent statutory officer, and the Commissioner and his or her staff are experts in the field of privacy. It makes sense to bring to bear that independence and expertise in the development of codes of practice. The process of making

530 *Necessary and Desirable* para 6.2.4. The fact that no code has been made under the Privacy Act for the banking and insurance industries could be due in part to the oversight of these industries by the Banking Ombudsman and the Insurance and Savings Ombudsman, established in 1992 and 1995 respectively.

codes of practice is a very public one. The intention to issue a code must be publicly advertised, and submissions on draft codes must be called for and considered. Codes must be publicly notified and made publicly available.

7.60 Nor do we think that the scope of codes of practice should be more restricted. The power to modify the effect of the privacy principles "up or down" provides a desirable degree of flexibility in the Act. While comparable overseas jurisdictions have more limited code-making powers, we do not regard the New Zealand provision as excessive.

7.61 In its submission to the Privacy Commissioner's 1998 review, the New Zealand Law Society observed:[531]

> A huge amount of work, time and resources goes into developing a code of practice. The effect of this expense is seen in the small number of codes that have been drafted. Industries perceive minimal benefits to their consumers, the costs of drafting a code appear to outweigh the benefits. The result is an inaccessible and ineffective code mechanism.

7.62 In the light of our assessment above, we do not think that this was a fair assessment of the code mechanism then, nor is it now. We note that the Privacy Commissioner did not recommend significant changes to the code of practice procedure in *Necessary and Desirable*.[532] In response to suggestions that codes of practice could be developed more quickly and efficiently, and that codes could be simpler and shorter, the Commissioner emphasised the status of codes of practice as pieces of delegated legislation, which alter the legal obligations imposed under statute.[533] They must therefore be issued with the precision expected of legislation and remain within the powers conferred by the Act on the Commissioner. We agree that the "code-lite" approach is not appropriate, and indeed propose below that the status of codes justifies their being made in the same way as ordinary statutory regulations.

7.63 We note that the work involved on the part of the OPC in developing and consulting on a code is very extensive for a small organisation. The early development of some of the codes now in place was hindered by a lack of resources. There is a suggestion that this may still be a problem, and that it is a factor in agency decisions not to invoke the code mechanism. For example, the Ministry of Education identified a code of practice as an alternative to the enactment of Part 30 of the Education Act authorising the use of the National Student Number (NSN). The Regulatory Impact Statement for the Education Amendment Bill 2004 (enacted as the Education Amendment Act 2006) makes the following observation about the code of practice option:[534]

> Authorisation Option A – Code of practice under Privacy Act 1993
>
> A code of practice under the Privacy Act 1993 would provide the authorisation of the extension for the NSN, specify permitted purposes and agencies permitted to use the

531 Quoted in *Necessary and Desirable* 207.

532 *Necessary and Desirable* Part VI.

533 See for example *Necessary and Desirable* para 6.2.6.

534 Ministry of Education "Regulatory Impact Statement Relating to the National Student Index", available at www.minedu.govt.nz (accessed 11 February 2010).

> NSN. A code would be subject to the complaints and damages provision in the Privacy Act 1993. A code is not the preferred option as it cannot establish penalties for misuse alone, nor require the compulsory use of the NSN by agencies. A code does not provide the same opportunity for parliamentary debate and decision-making that is desirable for such a widely applied identifier for a compulsory activity, and the centralised collection of personal information associated with the NSN. The development of the code would be managed by the OPC, including consultation. The work programme is determined by the OPC, which is experiencing resource constraints, and this creates some uncertainty for other projects requiring confirmation about the availability of the NSN.

7.64 The OPC is now better resourced than when it was first established, but our own involvement on the reference group participating in the review of the CRPC gives us some appreciation of the large amount of work involved in developing and maintaining a code.

7.65 Despite our general conclusion about codes of practice, we remain keen to find out whether or not any changes to the Act are required to make the development of codes more effective, or to improve the effectiveness of codes generally. We have not identified any ourselves. We welcome views.

Codes of practice enacted as ordinary regulations

7.66 As we noted above, we are happy with the majority of the code-making provisions and the processes they provide for, but we do consider that added constitutional safeguards should be added to the code-making process.

7.67 The code-making provisions in the Privacy Act confer considerable power on the Privacy Commissioner. In constitutional law terms, section 46 of the Act is a "Henry VIII" clause as it confers delegated authority to amend an Act of Parliament.[535] This sort of power should be granted by Parliament "rarely and with strict controls".[536]

7.68 Others have identified this issue as well. We note the submission from the Commonwealth Press Union to the Privacy Commissioner in the context of the *Necessary and Desirable* review:[537]

> The provision of codes where specific needs arise is one of the more useful pieces of flexibility available to affected industries or activities under the Act. We note, however, the wide powers of the Privacy Commissioner in drafting, accepting and amending codes of practice. There are significant constitutional issues in giving unelected officials such as the Privacy Commissioner the right to put in place codes which are potentially more restrictive than the law itself.

535 For more on Henry VIII clauses see Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2001, most recently amended 2007) 205–206.

536 Regulations Review Committee *Report on the Inquiry into the Resource Management (Transitional) Regulations 1994 and the principles that should apply to the use of empowering provisions allowing regulations to override primary legislation during a transitional period* [1995] AJHR I16C.

537 Quoted in *Necessary and Desirable* 203.

7.69 Moreover, as well as being Henry VIII provisions, codes do not follow the conventional process for regulation-making in New Zealand. As we noted previously, codes of practice are "deemed regulations". Ordinary regulations are drafted by the Parliamentary Counsel Office, approved by the Cabinet, made by the Governor-General in Executive Council, notified in the *Gazette*, and published in the Statutory Regulations Series (SR Series) and on the New Zealand Legislation website. Codes of practice, while they are deemed regulations, do not follow this process. Once issued by the Privacy Commissioner, codes have to be presented to the House of Representatives, can be examined by the Regulations Review Committee, and are subject to disallowance (and amendment) under the Regulations (Disallowance) Act 1989. As noted above, the Regulations Review Committee has examined one code of practice and identified issues with it.[538] It was of the view that changes were required, and these were subsequently made to the Committee's satisfaction.

7.70 Having accepted that the breadth of the power to make codes of practice is appropriate, we consider that accountability for the exercise of that power should be brought more into line with established constitutional arrangements. Ordinary regulations are made by the Executive, which has the confidence of the House and is answerable to it. As the Law Commission suggested in its submission to the Regulations Review Committee's examination of deemed regulations, "the further the law-making power is removed from Parliament and the greater its effect, the more 'constitutionally obnoxious' it becomes."[539]

7.71 In making this suggestion, we do not mean to imply that the Privacy Commissioner has in any way abused the powers conferred by the Act. Indeed, the Privacy Commissioner clearly recognises the significance of the powers, and goes out of her way to ensure that the process of code development is open and transparent, and that the final product of a high standard and readily accessible.

7.72 We note that the RRC recommended that all deemed regulations be approved by the Cabinet as part of the promulgation process, and that the Government Response to the RRC's report rejected this recommendation.[540] One of the primary concerns of the RRC in making this recommendation was related to quality assurance. The rejection of that recommendation in the Government Response was based on the inappropriateness of Cabinet processes simply as a quality assurance check. Our recommendation is based on more fundamental constitutional considerations.

538 See discussion of the Telecommunications Information Privacy Code above.

539 Law Commission "Submission to the Regulations Review Committee Review of Deemed Regulations". Noted as submission 30 to the Regulations Review Committee "Inquiry into Instruments Deemed to be Regulations – An Examination of Delegated Legislation" (Wellington, 1999) fn 30.

540 See *Government Response to the Report of the Regulations Review Committee on its Inquiry into Instruments Deemed to be Regulations – An Examination of Delegated Legislation* (October 1999); see also *Further Government Response to the Report of the Regulations Review Committee on its Inquiry into Instruments Deemed to be Regulations – An Examination of Delegated Legislation* (November 2000).

Model process

7.73 The sort of model we have in mind is the one incorporated in the Heath and Disability Commissioner Act 1994. Under that Act, the Health and Disability Commissioner (HDC) is required to develop a Code of Health and Disability Services Consumers' Rights (CHDSCR).[541] Notification and consultation obligations similar to those contained in the Privacy Act apply to the development of a Code by the HDC.[542] But while the Commissioner proposes, Cabinet disposes. Once a draft Code has been developed, the HDC forwards it to the Minister, who must present it to the House.[543] However, the Code does not become operative unless it is prescribed by regulations made under section 74 of the Act. The same process applies to amendments to the Code.

7.74 Indeed, it is possible under the Health and Disability Commissioner Act for the Executive to make regulations prescribing a CHDSCR that differs from the draft developed by the HDC, or contrary to or without the HDC's recommendations. But in that case the Minister must, within 12 sitting days of the making of the regulations, present a statement to the House explaining how the Code differs from that recommended by the HDC, and the reasons for the differences, or (where applicable) the reasons why the regulations were made contrary to or without a recommendation of the Commissioner.[544]

7.75 While this model is generally worthy of presentation here it is not entirely appropriate for codes of practice under the Privacy Act. A CHDSCR needs to be in place for the Heath and Disability Commissioner Act to work. So the option of prescribing a code that has not been recommended by the HDC has to be available to the Executive. Codes of practice are not essential to the operation of the Privacy Act.

7.76 Given the fact that privacy codes of practice can override the Privacy Act, and the importance of consultation in their development, we do not think that the Executive should be able to prescribe a code of practice in relation to a particular area unless the Privacy Commissioner has developed a code for that area and made a recommendation to the Government. The Government should be able to reject the proposed code, but not modify it.[545] If the Government were to reject the code, the Minister should have to give reasons to the House.

7.77 We do not see that the proposed new process should significantly affect the existing processes of code development and consultation. In effect, it gets the best of both worlds. It preserves the independence of the Privacy Commissioner, but imposes a greater degree of accountability for the exercise of the legislative function under the Act. There are some potential risks. We have considered whether the proposed new process might jeopardise meaningful participation by industry players in the code development process, and therefore adversely affect the quality of the outcome. The fact that the ultimate power to decide

541 Health and Disability Commissioner Act 1994, s 19.

542 Health and Disability Commissioner Act 1994, s 23.

543 Health and Disability Commissioner Act 1994, s 19.

544 Health and Disability Commissioner Act 1994, s 75.

545 The House of Representatives could still amend or replace the code, once incorporated in regulations, through the power conferred by section 9 of the Regulations (Disallowance) Act 1989.

whether a code is implemented or not would lie with the Executive, with the attendant risk that the effort that goes into the development of a code might be wasted if a code is rejected, might discourage engagement. We think that the robustness of the code development process, and the status of the Privacy Commissioner, make this unlikely, but we seek comments on the issue.

7.78 A further risk is that, despite the huge effort that goes into the development of a code, internal government processes might derail a proposed code if officials inappropriately seek to relitigate or second-guess the Privacy Commissioner's recommendations. Again, we think this unlikely, given that the Executive would only be able to reject a proposed code, and would have to give reasons publicly for the rejection.

7.79 The process we recommend would also mean that codes of practice would be published in the SR Series and on the New Zealand Legislation website. We think that the potentially broad application of codes of practice makes that entirely appropriate. This of course would not prevent the Privacy Commissioner from publishing annotated versions codes with explanatory and guidance material included, as the Commissioner does now.

Time limits on codes

7.80 There is one other change to the code-making procedure that we suggest should be considered. It also arises out of a constitutional issue. As indicated above, codes of practice are made under what amounts to a Henry VIII clause. The Regulations Review Committee (albeit in a different context) has recommended that regulations made under Henry VIII clauses should expire after a certain period (that is, there should be a sunset clause).[546] Section 46 of the Act provides that a code may provide for its review by the Commissioner, and may also provide for the expiry of the Code. Neither a review nor expiry are mandatory. We invite comment on whether or not they should be.

Significant policy issues

7.81 The ambit of the Privacy Act is very wide, covering personal information practices in most areas of the public and private sectors. Codes of practice can have a correspondingly wide application. The flexibility that codes of practice provide to address difficulties in the application of the Act or new issues that arise is, in our view, essential. However, this does not mean that a code of practice will always be the most appropriate way of dealing with an issue. There are some issues that, even though they could be dealt with by a code of practice, might be too contentious or significant to be legislated for in a code. Choosing the right instrument to deal with the issue is important. Although the code of practice process involves significant public input and consultation, sometimes legislation will be more appropriate.

546 Report of the Regulations Review Committee *Inquiry into the Resource Management (Transitional) Regulations 1994 and the Principles that Should Apply to the Use of Empowering Provisions Allowing Regulations to Override Primary Legislation During a Transitional Period* [1995] AJHR I16C.

7.82 The National Student Number issue mentioned above is a possible example.[547] In that case, the Ministry of Education noted that, although a code of practice could be used to authorise the extension of the NSN, "a code does not provide the same opportunity for parliamentary debate and decision-making that is desirable for such a widely applied identifier for a compulsory activity, and the centralised collection of personal information associated with the NSN". In the context of the TIPC, the Regulations Review Committee objected to the inclusion of certain provisions in the original code on the basis that that the enforcement of foreign laws should not be facilitated through a privacy code.

7.83 It is clearly impossible to identify in advance what issues might, or might not, be suitable to be dealt with in a code. However, our suggested change to the way in which codes of practice are implemented would assist in addressing this issue. The last word on implementing a code of practice would rest with the Government of the day, rather than the Privacy Commissioner. Cabinet could decide that, even though the Privacy Commissioner has developed a code of practice, a code is not the appropriate mechanism for dealing with the issue, and decline to prescribe the code.

CONCLUSION

7.84 Our overall conclusion is that the code of practice mechanism in the Privacy Act appears to be working satisfactorily. Nevertheless, we welcome comment and feedback on these issues.

Q94 Are any changes to the Act required to make the development of codes of practice more effective, or to improve the effectiveness of codes generally?

Q95 We consider that codes of practice should be implemented by ordinary regulations approved by Cabinet, rather than simply being issued by the Privacy Commissioner. Do you agree?

Q96 Should reviews, or sunset provisions, be mandatory in relation to codes of practice?

547 See paragraph 7.63 above.

Chapter 8

Complaints, enforcement and remedies

8.1 This chapter examines the complaints system under the Privacy Act and considers whether the existing approach is sufficient, or whether new enforcement tools and remedies are needed.

8.2 The essential aim of the existing Privacy Act is to secure voluntary compliance with the law through providing education, guidance, assistance and incentives to comply, backed up by the possibility of enforcement action in the event that voluntary compliance fails. This theory is often known as compliance-oriented regulation.[548] In it, non-punitive enforcement methods are used as the first step.

8.3 It is important to understand that the privacy principles in the Act are not enforceable in the courts.[549] Instead, breaches of the principles are dealt with through the complaints process established in Part 8 of the Act. There is an important exception. Access to personal information in principle 6, where the information is held by a public sector agency, is a legal right and that right is enforceable in the courts.[550] So far as we can find, however, there appear to be no decided cases in which claimants have sought to enforce their access rights directly in the courts.

548 See further Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 238.

549 Privacy Act 1993, s 11(2).

550 Privacy Act 1993, s 11(1).

OVERVIEW OF THE CURRENT SYSTEM

Complaints to Privacy Commissioner

8.4 Any person may make a complaint to the Privacy Commissioner alleging that any action is or appears to be an interference with the privacy of an individual. For the purposes of a complaint, an action is an interference with the privacy of an individual if it breaches a privacy principle, a code of practice, or Part 10 of the Act (relating to information matching). Furthermore, an action is not a breach of privacy unless it:[551]

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

Complaints about breaches of principles 6 and 7 do not require harm to be shown. There are some other special statutory jurisdictions, most notably section 22F of the Health Act 1956, which deem matters to be within the complaints jurisdiction.

8.5 The Act provides that in the performance of his or her functions, the Commissioner must have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.[552] This may also affect the interpretation of what amounts to a breach of privacy. The New Zealand Bill of Rights Act 1990 is a further influence.

8.6 The Commissioner usually receives around 600 to 700 complaints each year. In the 2008/2009 year there were 806, a significant increase.[553] Currently around 80 per cent are dealt with within six months. Complaints most commonly relate to denial of access to personal information requested under principle 6, and disclosure of personal information in breach of principle 11. Complaints about breaches of the other principles are much less common.[554] The Commissioner's functions in relation to complaints are to investigate, act as a conciliator and take such further action as is contemplated by Part 8 of the Act (that is, investigation and settlement of complaints, and action in the Human Rights Review Tribunal).[555]

551 Privacy Act 1993, s 66.

552 Privacy Act 1993, s 14(a).

553 Office of the Privacy Commissioner *Annual Report 2009* (Wellington, 2009) 25.

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

555 Privacy Act 1993, s 69.

Process

8.7 Upon receiving a complaint, the Office of the Privacy Commissioner (OPC) will assess it against the privacy principles in order to identify the issues involved in the complaint and determine the immediate direction of the investigation. They would then generally contact the complainant, and the respondent agency may also be notified of the complaint and asked to respond. Once the respondent agency has been notified, the matter becomes jurisdictionally qualified as one that could be heard by the Human Rights Review Tribunal.[556]

8.8 The Office would then consider a range of options to deal with the complaint, ranging from equipping the parties to resolve the issue themselves, to mediation or a full investigation of the complaint. Often further information is required from one or both parties. Previously, in the early stages complaints were handled by an Assessment and Conciliation Team, whose focus was on trying to resolve the complaint early. Where this team was unable to resolve a complaint, or the complaint was complex or difficult, it was referred to an Investigating Officer Team. In 2009, however, the Office trialled a one-team approach, where the same team undertook both work-streams. This meant that all the team was able to advance early settlement, rather than only half as before. The trial was a success.

8.9 When a complaint is investigated, the officer dealing with it will gather and analyse the facts about the complaint. At this stage the Office will begin forming an opinion about whether there has been a breach of the privacy principles and whether any harm has resulted from the breach. Where the Commissioner believes that the complaint has substance, the Commissioner must use his or her best endeavours to secure a settlement between the parties.[557]

8.10 The Office will generally attempt to resolve the dispute at all stages of the process. In most cases, either complaints are settled or complainants decide not to pursue the matter further after the investigation is completed.[558] Sometimes during the investigation investigating officers may indicate a legal view of the complaint in an attempt to persuade one or both parties of the merits of the case, with a view to encouraging settlement. If settlement does not occur, a more formal legal opinion may be given and a decision made as to whether to refer the complaint to the Director of Human Rights Proceedings ("the Director"). Parties are given an opportunity to respond before any adverse opinion is issued about them.

8.11 If a complaint cannot be settled, the Commissioner may refer the matter to the Director for the purpose of deciding whether proceedings should be instituted.[559] Over the last four years, the Commissioner has referred an average of 15 complaints each year to the Director.[560] A decision to refer the complaint to the

556 *L v T* (1999) 5 HRNZ 30 (HC); *Waugh v New Zealand Association of Counsellors Inc* (17 March 2003) HRRT 9/03.

557 Privacy Act 1993, s 77(1)(a).

558 Katrine Evans "Show Me the Money: Remedies under the Privacy Act" (2005) 36 VUWLR 475. In 2008–2009 the number of complaints settled or mediated rose by 43 per cent: Office of the Privacy Commissioner *Annual Report 2009* (Wellington, 2009).

559 Privacy Act 1993, s 77.

560 Office of the Privacy Commissioner *Annual Report 2008* (Wellington, 2008). In the 2008–2009 year the number referred was 12, down from 20 the previous year: *Annual Report 2009* (Wellington, 2009).

Director would only be made if the investigation has established an interference with the privacy of an individual. Credible and admissible evidence is required. Other factors such as the attitude of the parties, the seriousness of the breach, the possibility of relief from the Tribunal and other mitigating or aggravating features are also weighed.

Director of Human Rights Proceedings process[561]

8.12 When referring a complaint to the Director, the Commissioner sends a letter of notification together with a certificate of investigation. The certificate summarises the nature of the complaint, the key points and the statutory provisions that are in issue. The Director also receives the Commissioner's opinion that has been given to the complainant. Aside from this, however, the Director does not generally receive any further information about the complaint.

8.13 The Director then considers the complaint afresh in order to decide whether to begin proceedings in the Human Rights Review Tribunal ("the Tribunal"). The Act does not specify how this process should work, nor does it give criteria to be taken into account in deciding whether to begin proceedings. It provides that it is for the Director to determine, in his or her discretion, whether a matter justifies the institution of proceedings and whether proceedings should be instituted.[562] The only requirement is that the Director must give respondents an opportunity to be heard before instituting proceedings against them.[563]

8.14 The current Director draws on the Human Rights Act 1993, which has quite specific provisions. As a first step, he meets with respondents to give them the opportunity to explain why proceedings should not be issued. Often the response will be referred to the complainant for comment. Settlement offers are often made during this process and a considerable number of cases are settled at this point.

8.15 After hearing from the parties and considering the facts the Director then decides whether to bring proceedings. In making this decision, the Director often considers the following factors:

- whether there is a significant question of law involved;
- whether it would be an effective use of his resources to issue proceedings;
- the likelihood of success;
- the degree of harm to the complainant as a result of the interference with his or her privacy; and
- whether a reasonable settlement offer has been made.

8.16 If the Director decides to take the case, he would then notify the parties and begin proceedings in the Tribunal. Remedies sought would usually include a declaration of breach, an order preventing further breaches, an order that specific steps be taken to prevent further breaches, compensation and costs. The Director acts as the plaintiff, rather than appearing for the complainant.[564]

561 See generally Robert Hesketh "The Role and Function of the Director of Human Rights Proceedings in Cases Under the Privacy Act 1993" (Privacy Issues Forum, Wellington, 30 March 2006).

562 Privacy Act 1993, s 77(3).

563 Privacy Act 1993, s 82(3).

564 Privacy Act 1993, s 82.

8.17 Currently, the Director receives around 30 to 40 cases each year under the Privacy, Human Rights, and Health and Disability Commissioner Acts. Privacy cases are the most common, and have increased significantly since 2002.

Human Rights Review Tribunal process

8.18 Proceedings in the Tribunal may be brought by the Director, as outlined above, or by an individual. An individual may himself or herself bring proceedings if the Commissioner or the Director is of the opinion that the complaint does not have substance or ought not to be proceeded with, or where the Director agrees to the individual bringing proceedings or declines to take proceedings.[565] In such cases the Director may appear as an intervener, to independently assist the Tribunal.[566] An agency does not itself initiate proceedings.[567]

8.19 Cases in the Tribunal are by way of rehearing: the Tribunal considers the matter afresh. Again, the Act and Regulations[568] do not provide much guidance as how Tribunal proceedings should be conducted. There are uncertainties around the Tribunal's powers: for example, it is not clear whether it has the power to order discovery. In practice, the Tribunal operates in a similar way to a court, with a statement of claim, discovery and pleadings. Parties may call evidence and cross-examine witnesses.[569]

8.20 If the Tribunal is satisfied on the balance of probabilities that any action of the defendant is an interference with the privacy of an individual, it may grant one or more of the following remedies:[570]

- a declaration that the action is an interference with the privacy of an individual;
- an order restraining the defendant from continuing or repeating the interference or from engaging in, or causing or permitting others to engage in, conduct of the same kind as that constituting the interference;
- damages in accordance with section 88 of the Act (see below);
- an order that the defendant perform any act specified with a view to remedying the interference, or redressing any loss or damage suffered by the individual; or
- such other relief as the Tribunal thinks fit.

The Act provides that it shall not be a defence that the interference was unintentional or without negligence on the part of the defendant, but the Tribunal shall take the conduct of the defendant into account in deciding what, if any, remedy to grant.[571]

565 Privacy Act 1993, s 83.

566 Privacy Act 1993, s 86.

567 Katrine Evans "Show Me the Money: Remedies Under the Privacy Act" (2005) 36 VUWLR 475.

568 Human Rights Review Tribunal Regulations 2002.

569 Human Rights Review Tribunal Regulations 2002, reg 19.

570 Privacy Act 1993, s 85(1).

571 Privacy Act 1993, s 85(4).

8.21 The Tribunal has had around 17 new proceedings under the Privacy Act each year over the past five years. It issued 17 privacy decisions (including 10 interlocutory decisions on matters such as name suppression) during the 2008/2009 year.[572] Currently, Privacy Act cases comprise around half of its work.

8.22 As noted above, the Tribunal may award a range of remedies. The most commonly awarded remedies appear to be declarations and damages. Damages may be awarded in respect of any one or more of the following:[573]

- pecuniary loss suffered as a result of, and expenses reasonably incurred by the aggrieved individual for the purpose of, the transaction or activity out of which the interference arose;
- loss of any benefit, whether or not of a monetary kind, which the aggrieved individual might reasonably have been expected to obtain but for the interference; or
- humiliation, loss of dignity and injury to the feelings of the aggrieved individual.

The Tribunal may award damages of up to $200,000.[574] The highest award of damages so far has been $40,000.[575] Generally, awards are below $5000, although it has been suggested that large awards may be becoming more common.[576]

8.23 The Tribunal has developed some guidance about factors that it will consider in determining the level of damages. The approach may vary somewhat according to which principle is in issue. In *Hamilton v The Deanery 2000 Ltd*,[577] which related to principle 11, the Tribunal set out the following relevant factors:

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

8.24 If a complainant is not satisfied with the Tribunal's decision, there is a general right of appeal to the High Court.[578] There may be a further appeal with leave, on a question of law, from a decision of the High Court.[579]

---

572 Office of the Privacy Commissioner *Annual Report 2009* (Wellington, 2009) 33.

573 Privacy Act 1993, s 88(1).

574 Human Rights Act 1993, s 92Q.

575 *Hamilton v The Deanery 2000 Ltd* (29 August 2003) HRRT 36/02.

576 Katrine Evans "Show Me the Money: Remedies Under the Privacy Act" (2005) 36 VUWLR 475, 486; Katrine Evans "The Rise and Rise of Damages Awards for Breaches of Privacy? Hamilton v The Deanery 2000 Ltd" [2003] PLPR 56.

577 (29 August 2003) HRRT 36/02.

578 Human Rights Act 1993, s 123.

579 Human Rights Act 1993, s 124.

RATIONALE FOR THE COMPLAINTS PROCESS

8.25 The complaints process is modelled on the Ombudsmen and Human Rights Acts. Complaints are to be made to an independent and specialist entity, the Privacy Commissioner. The Act emphasises low-cost, non-adversarial and timely resolution of complaints.[580]

8.26 Parliamentary debates on the Privacy Bill indicate that the complaints process was intended to provide speedy and informal resolution of complaints wherever possible. The priority was to be to achieve a resolution through mediation, and the Tribunal (then known as the Complaints Review Tribunal) was a last resort, to be used when conciliation had failed.[581]

8.27 The key advantages of a complaints system are well stated in the Ministry of Justice's submission on the Privacy Commissioner's review of the Act:[582]

> A complaints procedure is clearly the most accessible and barrier free approach to seeking redress. The trade off for such an open mechanism is that the screening out of insubstantial complaints is difficult and resource intensive. In comparison the cost and procedural barriers of litigation in the general Courts usually provides a filter that prevents frivolous grievances progressing further, but at the same time may prevent deserving complainants from seeking redress.

8.28 Another advantage of a complaints-based system is that complaints can highlight deficiencies in systems. The Privacy Commissioner can then work with agencies to improve their systems, so that fewer breaches occur in the future. The courts cannot do this.

WHAT ARE THE PROBLEMS?

8.29 The system that we have described above appears to the Law Commission generally to be sound and working well. The process is highly effective in settling the vast majority of complaints. It is therefore a serious issue whether the policy parameters should be disturbed at all.

8.30 We have had the opportunity of conducting lengthy discussions with the Commissioner and her staff over a period of months. We have come to the conclusion that there are elements of the current process that are cumbersome. We think the process could be streamlined and made more efficient.

8.31 In particular, the structure and allocation of responsibilities between the Privacy Commissioner, the Director of Human Rights Proceedings and the Human Rights Review Tribunal, all making fresh assessments on the same set of facts, seems to us to be unnecessarily cumbersome. Furthermore, it causes delay and unnecessary expense.

8.32 There is a further problem. Currently, the system relies entirely on the complaints process to enforce compliance with the Privacy Principles. There are no further enforcement mechanisms. While the complaints process has been effective in providing redress in individual cases, it is not as effective as a method of

580 *Necessary and Desirable* 268.

581 (20 April 1993) 534 NZPD 14729.

582 Cited in Office of the Privacy Commissioner *Review of the Privacy Act 1993: Complaints and Investigation Submissions* (Wellington, 1998) 8.

promoting compliance with the Act as a whole. Neither is it good at addressing systemic issues that may exist in a particular organisation or industry practice as opposed to an isolated incident that can be the topic of a complaint.

REFORM

8.33 To address these problems we have developed proposals for reform, which we outline below. These proposals have been developed in consultation with the Office of the Privacy Commissioner. We have considered a wide range of options. We do not detail all the options considered here, but rather present what at this stage we believe to be the best option. We emphasise that at this stage we are not making firm recommendations, but rather proposals on which we seek feedback.

Aims of reform

8.34 Our reform proposals aim both to preserve the most effective features of the existing practice and to address the key problems noted above by making the dispute resolution and redress role more effective and more streamlined, and providing enforcement mechanisms to address systemic problems and encourage compliance.

8.35 The aim must be to encourage voluntary compliance so far as possible. Nevertheless, some sanctions for non-compliance are necessary in the Law Commission's view. Similarly, there needs to be redress for people harmed by breaches of the Act.

8.36 In our view, the reforms described in this section should:

- continue to provide cost-effective dispute resolution;
- maintain alternative dispute resolution methods to deal with the bulk of the complaints outside the court system;
- more efficiently dispose of small disputes that have no significant public aspects;
- deliver speedier outcomes where possible;
- make the transition from the alternative dispute resolution methods at the beginning of the process to the formal determination stage later easier;
- provide a more effective enforcement pyramid (that is, provide an escalating range of sanctions, beginning with education and persuasion to encourage voluntary compliance and escalating to sanctions in the event that voluntary compliance fails);
- provide a better means of ensuring systemic change;
- diminish some of the negative aspects of a complaints-driven system and provide scope for the Privacy Commissioner to redeploy her investigative resources in areas of broader public interest and importance; and
- meet international expectations.

Description of proposed reforms

8.37 Essentially, we propose a reformed complaints process together with some new enforcement tools. Our proposal has several key planks. First, we propose that the harm threshold for complaints should be removed. Secondly, we propose that the Commissioner be given the power to determine complaints under principle 6. The Tribunal would become an appeals body in cases involving principle 6. Thirdly, the role of the Director would be removed in all privacy complaints. Finally, the Commissioner would have a new power to issue enforcement notices where an agency is breaching the Act.

8.38 We outline below the key elements of the proposal, under the headings of dispute resolution, and compliance and enforcement. The proposed system is illustrated in Figure 1 below.

8.39 It is important to note at the outset that the Director and the Tribunal not only have jurisdiction over complaints under the Privacy Act but also deal with complaints under the Human Rights and Health and Disability Commissioner Acts. Our proposals involve changes only to the ways in which Privacy Act complaints are handled.

Dispute resolution

Reformed complaints process

8.40 We believe that the current system for complaints to the Privacy Commissioner should be maintained, with some adjustments to make it work better.

8.41 One major change we propose to the complaints process is to remove the requirement in section 66 that there must be harm (or potential harm) in order to make a complaint. Rather, the degree of harm suffered by the complainant will be a factor taken into account in the exercise of discretions such as whether to continue an investigation or refer a complaint to the Tribunal, and in determining what, if any, remedies to award.

8.42 The harm threshold is intended to filter out less deserving cases, but this works imperfectly. Some potentially worthwhile complaints are currently barred because no actual harm has yet occurred or become demonstrably likely, although there has been a breach of the Act which could conceivably cause harm in the future. Conversely, some comparatively trivial complaints are allowed because there is minor harm. We think that removing harm as an absolute bar to complaining would be easier for complainants to understand, allow more consistent enforcement of the Act, and be useful in exposing systemic problems where an agency or industry is breaching the Act but no harm has yet arisen. There is a risk that the Commissioner will receive large numbers of minor complaints where there is no harm, but we think that there are sufficient mechanisms in the Act to manage this.

8.43 The complaints process should be further fine-tuned through implementing recommendations previously made by the Commissioner.[583] We discuss several of the most significant of these in more detail later in this chapter. Some key aspects include:

- clarifying the ability to make representative complaints;
- new controls around intake and pursuit of cases; and
- enhanced procedures for getting matters before the Tribunal.

8.44 The Office will be likely to continue to seek to conciliate nearly all cases but will be increasingly reluctant to devote significant investigative resource to any complaints not raising systemic issues or otherwise raising issues of general importance (for example, novel issues or especially serious harm).

Access determinations

8.45 We propose a further change in the way complaints under principle 6, as well as equivalent provisions in codes of practice, are handled. In our view, these complaints, which we will term access reviews here,[584] should be determined by the Commissioner rather than the Tribunal. Complaints about breaches of all other principles, codes of practice or information matching would continue to be determined by the Tribunal if they cannot be settled. A Commissioner determination of an access case may be appealed to the Tribunal but, if not challenged in this way, would become binding and enforceable. For this category of complaints, then, the Tribunal would be recast as an appellate body.

8.46 There is a question as to whether complaints under principle 7 should also be handled in this way. The two principles of access to and correction of personal information often go together. There are, however, differences. A principle 6 complaint effectively involves a review of a file, the contents of which even the complainant does not know. It is essentially a review of an agency decision. Principle 7 complaints are not so much reviews as complaints about an agency's actions or failures to act. Moreover, what a determination under principle 7 would involve is less clear. Currently, an agency does not have to correct personal information, but only has to take such steps as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, a statement of the correction sought but not made.[585] The question, therefore, is whether, if the Commissioner could "decide" a principle 7 complaint, she would need power to order that the material actually be corrected. Currently, then, we confine our proposal to access complaints under principle 6.

583 *Necessary and Desirable* and supplements, recommendations 29, 37B, 58A, 66, 101A-101F, 102A, 103, 104, 104A, 105, 106, 107, 107A, 109, 110, 111, 112, 112A, 112B, 113B, 113C, 114, 115, 116A, 144, 146, 148, 149, 149A and 150.

584 "Access reviews" refers to complaints of refusal to give access to information, and could be extended to encompass all principle 6 cases (for example, failure to meet time limits).

585 See discussion in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, last updated 2007) PVA6.10(b), 6.10(d).

8.47 We would envisage that the Commissioner would be able to determine the complaint by making an order, for example that the personal information requested be made available. There would need to be provision for enforcement of such determinations. A possible method of enforcement could be through the Commissioner issuing an enforcement notice. We discuss our proposal for these notices later in this chapter. Another model could be the provisions of the OIA relating to the Ombudsmen's recommendations: departments are required to produce the relevant information as soon as reasonably practicable and no later than 20 working days after the day they receive notification. The organisation is under a public duty to observe the recommendation.[586] We anticipate that the complainant, and possibly also the Commissioner, would be able to seek enforcement of a determination.

8.48 The Commissioner's office may need to use a "Chinese wall" between staff working on investigation/conciliation and determination if the merits of alternative dispute resolution are to be maintained. There are models available for doing that. Another possibility would be to have a dedicated officer, such as an Assistant Commissioner, within the Office responsible for determinations.

8.49 There are several reasons why we believe this change would be beneficial. First, access cases make up about half of the Commissioner's complaints workload, so efficiencies gained here will assist significantly in making the system more efficient overall. The Ombudsmen have a similar jurisdiction in relation to access to official information.[587] Furthermore, although the statute uses the generic term complaints, complaints involving refusal to give access to information are really reviews of the agency's grounds for refusal. The Commissioner's office examines the relevant file and assesses whether the agency's decision complies with the Act. This is quite different from the way other complaints are dealt with, and lends itself to being resolved on the papers. Conversely, at present if the Commissioner cannot settle the matter the process must restart at the Tribunal stage. The Tribunal conducts an adversarial hearing and often does not examine the documents in issue until near the end of the hearing. This model is not well suited to access reviews.

Removing the Director of Human Rights Proceedings from the process

8.50 At present, the Act separates conciliation and litigation functions, so that the Commissioner's ability to conciliate is not undermined by also having an enforcement role. However, the separation seems to us to add unnecessary complexity and delay, causes confusion for complainants, and may also undermine the coherence of the specialist Privacy Commissioner model. We therefore propose that the Director no longer be involved in privacy cases. The current Director's functions would then be carried out by the Commissioner.

8.51 The Director currently performs a role similar to that of a Prosecutor, which we envisage the Commissioner would take over. That is, the Commissioner would act as the plaintiff in the Tribunal. The current power of the Director in section 20 to institute proceedings for a declaratory judgment would also vest in the Commissioner. These new responsibilities would require resources to deepen

586 Official Information Act 1982, ss 29A and 32.

587 Official Information Act 1982, Part 5.

the Office's litigation capability. It may be necessary to create a "Chinese wall" between staff involved in investigating or settling cases and those taking cases to the Tribunal, so as not to interfere with conciliation. Some overseas Privacy Commissioners operate this kind of system, as does the Office of the Health and Disability Commissioner.

8.52 We note again that the Director has other jurisdictions. We are concerned only with the Director's jurisdiction in privacy.

Human Rights Review Tribunal

8.53 We envisage that the Tribunal would have a new appeal jurisdiction in relation to access determinations and enforcement notices (discussed below). These appeals could be brought by the respondent or the complainant rather than only by complainants (through the Director or on their own motion), as happens now. Significantly, allowing the respondent to bring an appeal throws the onus back upon an agency subject to an adverse determination to comply with the obligation to do as the Act requires or else launch appeal proceedings. Under the current system, a non-complying agency can simply sit back and wait to see if the Commissioner, the Director or the aggrieved individual are serious about suing the agency and, if need be, settle at the eleventh hour. In the context of access the change in dynamics should work significantly in favour of promoting compliance, especially with uncooperative respondents.

8.54 Civil proceedings before the Tribunal to resolve complaints other than access reviews would remain much the same, albeit with some changes brought about through the refinements suggested in paragraph 8.43.

8.55 A greater portion of cases that do proceed would be appeals rather than the resource intensive de novo hearings under the current system. The change will play to the analytical legal strengths of the Tribunal.

8.56 A further important change we propose is to require that the Chair of the Tribunal be a District Court Judge. It is inappropriate that Chairs currently do not have security of tenure when they have a jurisdiction of such power and width. To exercise the powers of the Human Rights Review Tribunal without judicial independence is constitutionally unsound.[588] Although this proposal would affect all the Tribunal's jurisdictions, not only privacy, we think this an important reform.

588 See further New Zealand Law Commission *Tribunal Reform* (NZLC SP20, Wellington, 2008) 85.

8.57 We propose to strengthen enforcement through the introduction of an important new tool, the power to issue enforcement notices. This will provide greater powers to address non-compliance, as well as providing an incentive to comply voluntarily. Other proposals discussed in this paper should also provide more tools to enforce compliance with the Act. These include mandatory audit powers, discussed in chapter 6. The new power for the Commissioner to make determinations in access cases should also encourage compliance, because it more firmly places the onus upon agencies to comply or take steps to challenge a ruling of the Commissioner before the Tribunal, rather than being able to simply sit back and wait.

Enforcement Notices

8.58 The key reform we propose to the Act's enforcement machinery is to give the Commissioner power to issue binding enforcement notices. These would involve the Commissioner identifying a breach or breaches of the Act by an agency and requiring certain action within a specified period of time to comply with the Act.[589] We envisage that the respondent would be able to appeal to the Tribunal against a notice. If not appealed within a certain time, or appealed unsuccessfully, the notice would become enforceable, either in the Tribunal or in the District Court. If appealed, the matter would be considered in the Tribunal and disallowed or issued as a Tribunal order.[590] Models for this can be found in New Zealand statutes such as the Resource Management Act 1991 and in overseas privacy legislation.[591]

8.59 There would be consequences for failure to comply with a notice or order. We envisage that non-compliance with an enforcement notice would be an offence. There may be advantage in having escalating sanctions such as civil pecuniary penalties as well as offence provisions (including continuing offences). The enforcement pyramid works best when there is a prospect of escalating the sanctions.

8.60 Enforcement notices would not be contingent upon a complaint about the breach in question: if the Commissioner became aware of non-compliance, for example through an audit, he or she could issue a notice. The Commissioner's powers of inquiry under section 13(1)(m) could also be used to uncover breaches. Notification under a mandatory breach notification obligation (discussed in chapter 16) could be a further way to identify non-compliance. Indeed, one of the benefits of introducing enforcement notices is that they allow the Commissioner to enforce the Act where there is non-compliance but no complaints have been made.

589 See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) R50-1 for a similar recommendation.

590 The process has similarities to the abatement notice/order processes under the Resource Management Act 1991.

591 See, for example, Information Privacy Act 2000 (Vic), Part 6. See also UK Information Commissioner www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx for examples of enforcement notices that have been issued in the UK.

8.61 Notices might also be issued after investigation of a complaint. For example, if a complaint revealed a breach of the Act, and there was evidence of a systemic failure, the Commissioner could issue a notice. Using enforcement notices in the context of complaints would need careful consideration, because some might see them as cutting across the principles of the complaints process: that the Commissioner conciliates but cannot formally determine the complaint (although we have proposed to change this for access complaints). However, in reality there is no conflict: correcting an agency's behaviour, and resolving a complaint vis-à-vis the particular complainant, are not the same thing.

8.62 Enforcement notices could also be a useful tool in relation to enforcement of assurances given as part of a settlement of a complaint. The Act anticipates that assurances against repetition of the complained-about behaviour will often form part of a settlement.[592] However, currently the Act does not provide for enforcement if an assurance is breached. The Commissioner has previously recommended changes to the Act to allow action in the Tribunal where an assurance is breached.[593] Enforcement notices could be an alternative or additional means of enforcing assurances in particular cases, and if an agency then did not comply with a notice there would be consequences, as discussed above. Draft enforcement notices might be served on an agency and as a result a negotiated enforceable assurance might be agreed.[594]

8.63 Consideration will need to be given to how the decision to issue an enforcement notice should be made. The power to issue enforcement notices is a significant new power, and it is important that it be applied consistently. We would anticipate that criteria would be developed to guide decisions about when an enforcement notice is an appropriate response to a breach of the Act. The UK Information Commissioner has five key principles of transparency, accountability, proportionality, consistency and targeting to guide decisions about the exercise of powers including enforcement notices. The Information Commissioner's Office applies criteria including:[595]

- the seriousness of the detriment to an individual caused by a breach;
- whether so many people are affected that action is justified;
- whether there is a need to clarify an important point of law or principle;
- whether the breach is likely to have an ongoing effect or to recur;
- whether there is a need to set an example for a particular sector or activity;
- whether the cost to the agency of taking remedial action is reasonable;
- whether the agency has failed to follow relevant guidance or accepted business practice;
- whether the agency has taken a deliberate, wilful or cavalier approach;
- whether it would be more appropriate or effective for action to be taken by other means;
- the level of public interest in the case;
- whether taking action is an effective use of limited resources; and

592 See Privacy Act 1993, ss 74 and 77.

593 *Necessary and Desirable* recommendation 112.

594 See UK approach www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx (accessed 26 January 2010).

595 Information Commissioner's Office *A Strategy for Data Protection Regulatory Action* (2005).

- whether there is a risk to the credibility of the law or the Commissioner's office in not taking action.

We would expect some criteria of this type to be developed in New Zealand, whether they are developed by the OPC over time or established more formally.

8.64 Some further questions that will need to be considered are:

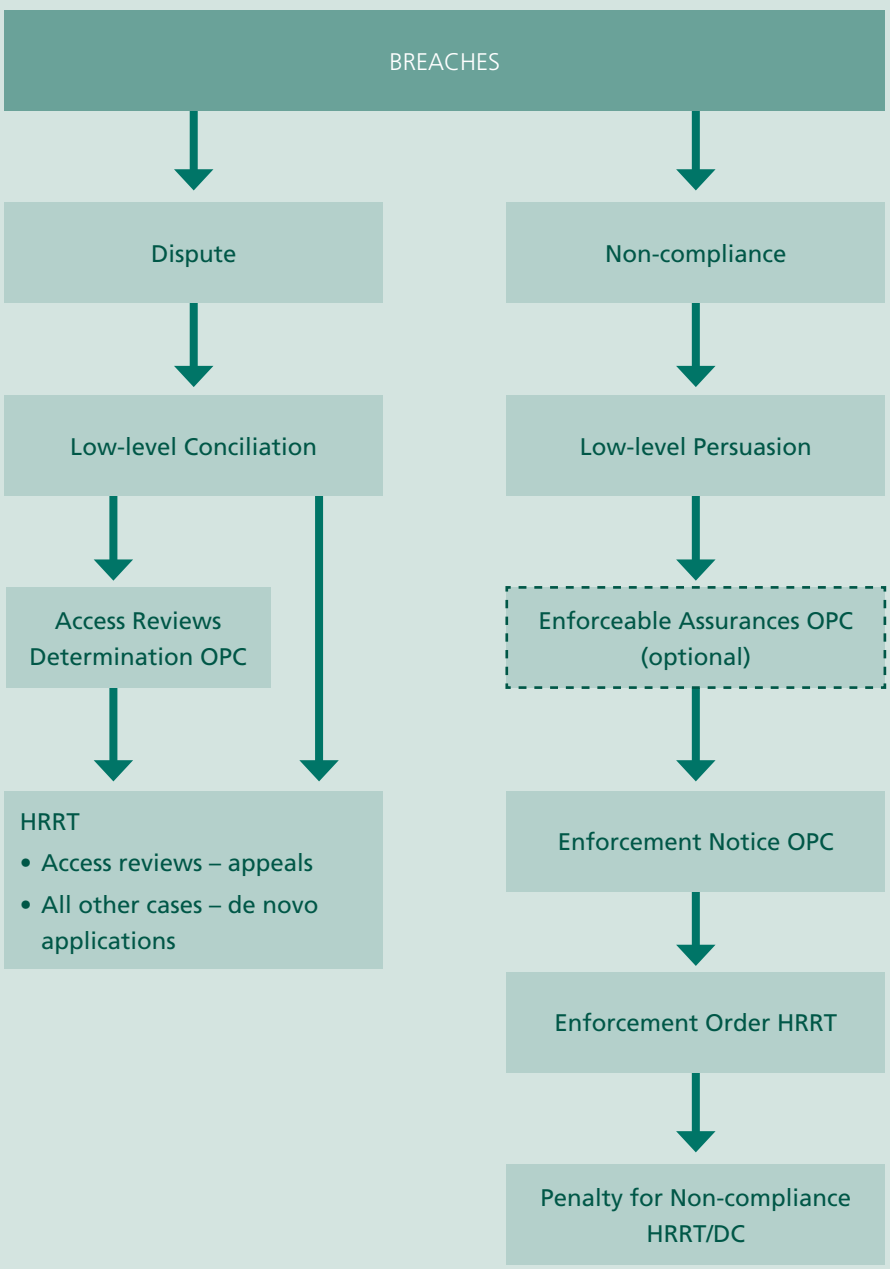
- Who would notices be issued to? That is, should they only be able to be issued to an individual agency or, if the Commissioner became aware of a systemic problem affecting an entire industry, could they be issued to a wider group?
- What evidence of breach would be required for the issue of a notice?
- If enforcement notices are to be available for complaints, how will it be determined when to use the power in relation to complaints?
- Should notices be enforced only by the Commissioner or should others (such as complainants if a notice is issued in relation to a complaint, or an individual or group seeking to enforce a notice in the public interest) also be able to take enforcement proceedings?

8.65 With the new enforcement model, the Office will probably give greater attention to assurances which will become enforceable. A monitoring regime would check adherence. Agencies may be more willing to give assurances and adhere to them because the alternative may be to have an enforcement notice issued.

8.66 The Office of the Privacy Commissioner would also develop proactive systems to identify non-compliance and not just wait for complaints. An enforcement strategy would be developed given the new range of enforcement tools. Monitoring of assurances would be strengthened. Public interest groups would see more point in drawing matters to the attention of the Office, as the Commissioner could take action without receiving an individual complaint. This enhancement of Office activities is particularly suited to the environment of the information revolution where issues of real concern may be largely invisible to the general public and therefore fail to generate complaints.

8.67 It is anticipated that there would be appropriate transparency for these enforcement processes. In the UK the Information Commissioner posts both assurances against repeated breach and enforcement notices on the Commissioner's website. Name and shame is a potent compliance weapon that is not yet used in the New Zealand context. An Office enforcement strategy would develop an approach to this which might also include naming respondents in serious dispute resolution cases.

FIGURE ONE


BREACHES
Dispute
Non-compliance
Low-level Conciliation
Low-level Persuasion
Access Reviews Determination OPC
Enforceable Assurances OPC (optional)
HRRT
• Access reviews – appeals
• All other cases – de novo applications
Enforcement Notice OPC
Enforcement Order HRRT
Penalty for Non-compliance HRRT/DC

Anticipated advantages of reforms

8.68 We see the key advantages of our proposals as streamlining the system and making it more efficient, promoting compliance with the Act, assisting the Commissioner's office to focus enforcement methods more effectively and improving public understanding of the system.

8.69 The suggested reforms should have an impact even before the Commissioner receives a complaint. The prospect of more serious enforcement of statutory obligations should influence management in agencies towards taking privacy and information security issues more seriously. Better voluntary compliance may result. Also when problems arise, or a consumer complaint is received, there may be a greater willingness to act quickly to take the appropriate remedial action. On the other hand, however, there is a risk that agencies might become less likely to admit breaches, knowing that there are greater enforcement powers available.

8.70 The introduction of stronger enforcement powers is likely to have a good effect on some recalcitrant respondents and facilitate further settlements.

8.71 The current system places the emphasis upon settling individual disputes. While we envisage that individual dispute resolution will continue to have a high priority, new tools will exist for exposing and addressing systemic issues.

8.72 Handling of complaints at the intake point would continue the current emphasis on seeking informal resolution where possible, quick responses rather than delayed, and investigation only where warranted. However, there will be a shift of emphasis at an early point to also identify and isolate the systemic and public interest features. This would be informed by an enforcement strategy developed in the Office of the Privacy Commissioner.

8.73 The complaints jurisdiction will move from allegations of an "interference with privacy" to simple allegations of a breach of the Act. Through this change it is anticipated that a broader spectrum of complaints will come before the Commissioner, including some having serious systemic aspects but limited actual harm to the individual complainant. Currently, cases where actual harm is not apparent or envisaged are prevented from entering the system.

8.74 There will also be a slightly broadened discretion to refuse to investigate or to discontinue cases, for example by excluding "stale" cases. More importantly, there would be a greater willingness to use the existing powers to end involvement in small cases where effective enforcement is being taken on the systemic issue. At the moment, there may be unwillingness by both the Office and complainant to "let go" of an unpromising complaint given that it is the only leverage available to address an issue. The enforcement powers should change the dynamic.

8.75 The main source of enforcement cases is likely to remain individual complaints. However, Commissioner-initiated inquiries would likely increase in number and significance, given that the outcome might include enforcement.

8.76 Finally, the new system should be better understood by complainants, with the question of harm raised not as an opening threshold issue, but rather when the OPC explores how best to pursue or finally dispose of the matter.

Q97 We propose that the complaints, enforcement and remedies provisions of the Privacy Act should be reformed in the manner outlined in paragraphs 8.33–8.76. Do you agree? In particular do you agree that:

- the harm threshold in section 66 of the Act should be removed;
- the role of the Director of Human Rights Proceedings should be discontinued for privacy cases;
- for access reviews the Privacy Commissioner should determine the complaint and the role of the Human Rights Review Tribunal should be that of an appellate body;
- the Human Rights Review Tribunal should be chaired by a District Court Judge;
- the Privacy Commissioner should be given statutory power to issue enforcement notices; and
- non-compliance with an enforcement notice should be made an offence?

Q98 Are any other dispute resolution or enforcement mechanisms required?

FURTHER ISSUES

8.77 This section discusses in more detail several of the Privacy Commissioner's previous recommendations, which we noted in paragraph 8.43, as well as considering the Ombudsmen's ability to review decisions on complaints under the Privacy Act.

Representative complaints

8.78 The Commissioner has made recommendations about representative complaints, by which we mean a complaint brought by a representative person or body on behalf of a group, all the members of which would be able to make complaints individually if they chose. The result applies to all the members of the group. The concept is similar to a class action in litigation.

8.79 As it stands, the Privacy Act does not prohibit representative complaints, and even contemplates them. Section 67(1) states that:

> any person may make a complaint to the Commissioner alleging that any action is or appears to be an interference with the privacy of an individual.

It seems that the person who makes that complaint and the individual whose privacy has allegedly been interfered with do not have to be the same person. The Commissioner does, however, have discretion to take no action if, in her opinion, the complainant does not have a sufficient personal interest in the subject-matter of the complaint.[596]

596 Privacy Act 1993, s 71(1)(e).

8.80 The provisions about action in the Tribunal specifically refer to class actions:[597]

> The Director of Human Rights Proceedings may, under subsection (2) of this section, bring proceedings on behalf of a class of individuals, and may seek on behalf of individuals who belong to the class any of the remedies described in section 85 of this Act, where the Director of Human Rights Proceedings considers that a person to whom this section applies is carrying on a practice which affects that class and which is an interference with the privacy of an individual.

Individuals can also bring cases to the Tribunal under section 83. It is not clear whether an individual could do so on behalf of a group.[598]

8.81 While on their face these provisions allow representative complaints, the Commissioner has recommended that consideration be given to providing more guidance in the Act for the registration and handling of representative complaints.[599] Currently, the Act gives no guidance on issues such as how a class should be established and how the proceedings should be handled. The Commissioner felt that the current provisions are unlikely to be used in the absence of more specific mechanisms in the Act.

8.82 It has been suggested that privacy breaches are well suited to resolution through representative action. Some reasons for this include:[600]

- In an ordinary complaint, the person who has suffered an invasion of privacy must identify him- or herself and allow the Privacy Commissioner to look into the facts, which could be seen as exacerbating the original loss of privacy. In contrast, in a representative complaint another person can do this, so these difficulties are mitigated somewhat.
- It provides more scope to address systemic issues. Some privacy breaches may appear minor to an individual, who might not bother to complain. However, the breach may in fact affect a large number of people or reveal a problem in an agency's practices. Complaints which may not be worthwhile for an individual to pursue may be easier to justify for a class.
- A representative complaint may provide a greater deterrent than an individual complaint. Representative complaints may have a higher profile and thus a greater risk that the agency complained about will attract negative publicity.
- There are practical benefits, such as spreading the costs of the complaint across a group.

597 Privacy Act 1993, s 82(4).

598 In *New Zealand Freedom from Discrimination Group v New Zealand Grand Lodge of Freemasons* (1984) EOC 92-008, the Equal Opportunities Tribunal did not resolve the question of whether a group of aggrieved persons could pursue a class action where the Human Rights Commission or Race Relations Conciliator declined to proceed on their behalf.

599 *3rd Supplement to Necessary and Desirable* para 2.13, recommendation 102A.

600 Chris Connolly and Nawaz Isaji "Representative Complaints – A New Approach to Making Privacy Laws Work for Consumers" (Paper presented to Surveillance and Privacy 2003 Conference, Sydney, 8–9 September 2003) 3–4.

8.83 Given these potential benefits, we think that the Act should provide more detail with regard to representative complaints. There are a number of options for how such complaints could work, and consideration would need to be given to questions such as:

- whether the representative (that is, the person who makes the complaint on behalf of the group) needs to be part of the affected group or whether an unaffected person could complain on behalf of others;
- whether the consent of the other members of the group should be required; and
- whether the group should be formed on an opt-in or opt-out basis – that is, whether members should have to affirmatively join the complaint or whether everyone affected by the relevant breach would be presumed part of the complaint unless they opted out.[601]

8.84 There are provisions in relation to representative complaints in the Privacy Act 1988 (Cth),[602] and these provisions could perhaps provide a model for clarifying how representative complaints are to be handled under the New Zealand Privacy Act.

Q99 Should the Act provide more specifically for the taking of representative complaints? If so:

- Should the representative be required to be personally affected by the alleged breach?
- Should the consent of other members of the group be required?
- Should the group be formed on an opt-in or opt-out basis?

Offences

8.85 The Privacy Commissioner has recommended that two new offences be added to the Act. The Commissioner noted that the Act is primarily enforced through civil remedies, rather than the criminal law, and that in general this approach is preferable to including a lot of criminal offences. However, the Commissioner felt that there was a case for introducing these offences because they related to wilful and unacceptable behaviour which the civil law was not capable of constraining.

601 In the UK, the Civil Justice Council has recently reviewed the law on collective actions in the courts. The report and government response contain some useful discussion about some of these points. See Civil Justice Council *Improving Access to Justice through Collective Actions* (2008); Ministry of Justice *The Government's Response to the Civil Justice Council's Report: 'Improving Access to Justice through Collective Actions'* (2009); Civil Justice Council *Draft Court Rules for Collective Proceedings* (2010).

602 Privacy Act 1988 (Cth), ss 38, 38A, 38B, 38C, 39. See also discussion in Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 1636–1638.

8.86 The first is an offence of intentionally misleading an agency by:

- impersonating the individual concerned; or
- misrepresenting the existence or nature of authorisation from the individual concerned;

in order to obtain personal information or to have that personal information used, altered or destroyed.[603]

8.87 This proposed offence would address the growing problem of "pretexting". The Commissioner recently noted that worrying practices have been exposed overseas, involving systematically misleading agencies to obtain personal information, which may then be traded.[604] Currently, an individual whose personal information has been exposed may be able to complain against the agency for disclosing the information or failing to keep it secure, but such a complaint may not succeed. There is no remedy against the person who engaged in deception to obtain personal information.

8.88 The second proposed offence is knowingly destroying documents containing personal information to which the individual concerned has sought access in order to evade an access request.[605] The Commissioner felt that it would be appropriate to create an offence for this conduct because the civil law response, which would be a complaint and a review of the reasons for refusing access, has been deliberately thwarted. If the information has been destroyed it would be almost impossible to evaluate a complaint. Furthermore, the Commissioner felt that deliberately denying people their entitlements is unacceptable conduct which ought not to be permitted.

8.89 There are international precedents for such offences.[606] We think that their inclusion in the Act is worth considering.

Q100 Should there be new offences of:

(a) intentionally misleading an agency by impersonating an individual or misrepresenting the existence or nature of authorisation from an individual in order to obtain personal information or to have personal information used, altered or destroyed; and/or

(b) knowingly destroying documents containing personal information to which an individual has sought access in order to evade an access request?

Q101 Should the Act contain any further offences?

603 *Necessary and Desirable* paras 12.16.5–12.16.8, recommendation 148.

604 *4th Supplement to Necessary and Desirable* para 2.22. See also Information Commissioner *What Price Privacy?* (London, 2006), exposing extensive illegal trade in personal information.

605 *Necessary and Deisrable* paras 12.16.9–12.16.12, recommendation 149; *1st Supplement to Necessary and Desirable* paras 3.9.1–3.9.6; *3rd Supplement to Necessary and Desirable* paras 2.22.1–2.22.3.

606 See, for example, Data Protection Act 1998 (UK), s 55; Personal Information Protection and Electronic Documents Act SC 2000 c 5, ss 8(8) and 28.

Ombudsmen reviews of the Commissioner's investigation of complaints

8.90 The Ombudsmen may investigate any decision or recommendation made, or any act done or omitted, relating to a matter of administration and affecting any person or body of persons in his, her or its personal capacity, by government departments and organisations including the Privacy Commissioner.[607]

8.91 Generally speaking, when the Ombudsmen investigate actions of the Privacy Commissioner they will be concerned with matters of process. But, potentially, an investigation could extend beyond this and enter into substantive matters. If the statutory language were clear and reasonably open to only one interpretation, then it would be open to the Ombudsmen to find that a different interpretation is incorrect. In such a case, they may form the view that an opinion of the Privacy Commissioner was based, either wholly or partly, on a mistake of law.[608] Even if there were more than one possible interpretation, they may still find that it was unreasonable in the context to adopt a particular interpretation. If this happened it could result in the Ombudsmen substituting their view of the correct interpretation of the Privacy Act for the Privacy Commissioner's view on a complaint.

8.92 It could, in other words, result in one agency substituting its view for that of another in what is effectively a quasi-judicial inquiry. We are interested to know whether there should be a narrower statutory definition of the Ombudsmen's power to investigate actions of the Privacy Commissioner, and indeed whether the Privacy Commissioner should be subject to the Ombudsmen Act at all.

Q102 Are any changes needed to clarify the Ombudsmen's role in investigating the Privacy Commissioner's handling of complaints under the Privacy Act?

Q103 Do you have any further comments on the Act's provisions regarding complaints, enforcement and remedies?

607 Ombudsmen Act 1975, s 13(1).

608 Ombudsmen Act 1975, s 22.

Chapter 9
Information matching

9.1 The State collects and holds a vast amount of personal information about its citizens. Some of the information is provided by citizens of their own accord. Most is acquired either by compulsion or in circumstances where a citizen has no choice but to provide the information if he or she wants to receive a service or benefit. And technology now provides the tools to use this huge store of information in ways never before possible. As one commentator has noted:[609]

> it has become practical to manage, exchange, match and mine vast quantities of information about people and their personal lives, rapidly and without their involvement. The technological capacity and the bureaucratic imperative to record and report that it facilitates have far outpaced social change. It is like the Black Death: the population has no natural resistance and no real understanding of what is happening and why.

9.2 This chapter and the next relate to information matching and information sharing. Both are matters that relate exclusively or principally to the activities of public sector agencies rather than the private sector. While the two matters have a significant degree of overlap, each raises quite distinct issues.

9.3 Information sharing (or data sharing) is a wider term than information matching. Information sharing covers the situation where information is made available by one agency to another. Information sharing is covered by the ordinary privacy principles (except where another statutory provision applies). One of the key issues raised in the next chapter is whether the privacy principles are sufficiently clear or flexible to enable the sharing of information between government agencies when this is necessary or desirable in the public interest or the interests of an individual.

9.4 Information matching (or data matching) is in some respects a subset of information sharing, since it involves one agency making information available to another. In some cases the ordinary privacy principles would not prevent it. However, information matching has its own regime in the Privacy Act. It is dealt

609 Submission by No2ID, quoted in Richard Thomas and Mark Walport *Data Sharing Review Report* (2008) Annex C 26.

with in Part 10 and Schedules 3 and 4. Information matching essentially involves "the comparison of one set of records with another, generally with the aim of finding records in both sets that belong to the same person."[610]

9.5 This chapter:

- looks at what information matching is, and why the Act contains a separate regime for it;
- examines the existing provisions in the Act and whether or not they are working in practice;
- looks at overseas approaches to information matching in Australia, Canada, the UK, the US, and Hong Kong, and whether there are any lessons to be learned; and
- puts forward a number of suggestions for change.

BACKGROUND What is information matching?

9.6 Part 10 and Schedules 3 and 4 of the Act relate to information matching by public sector agencies. Information matching essentially involves the (usually computerised) comparison of personal information from one source against personal information from another source, for the purpose of producing or verifying information about an identifiable individual. In most cases, the objective is to detect whether identifying information (usually a name) about the same individual appears in both sets of information. Occasionally, the fact that an individual's information appears in only one set of information will be of interest. An objective often associated with information matching is the detection of fraud in the delivery and receipt of social assistance programmes such as social welfare benefits and student allowances. However, in some cases the objective may be to benefit the individual, such as identifying people who are eligible to vote but are not registered as electors, or people who are not claiming a social welfare benefit to which they are entitled. Over the years since information matching was first legislated for in New Zealand, there has been a shift towards purposes that are more beneficial to individuals than the original purpose of detecting and avoiding benefit fraud.

9.7 The primary purposes of information matching have been identified as being:[611]

- detection of errors in programme administration;
- confirmation of continuing eligibility for a benefit programme, or compliance with a requirement for a programme;
- detection of illegal behaviour by taxpayers, benefit recipients, government employees, and so on;
- monitoring of grants and contract award processes;
- location of persons with a debt to a Government agency;
- identification of those eligible for a benefit but not currently claiming;
- data quality audit; and
- updating of data in one set of records based on data in another set.

610 Privacy Commissioner *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2009* (Office of the Privacy Commissioner, Wellington, 2009) 41.

611 Roger Clarke "Dataveillance by Governments: The Technique of Computer Matching" (1993), available at www.rogerclarke.com.

Why is information matching dealt with specifically in the Act?

9.8 Authorising the exchange of information between certain government agencies for the purpose of combating fraud and abuse of the social welfare system, and subjecting those information exchanges to a system of controls, reporting, and monitoring, was one of the purposes of the Privacy of Information Bill introduced in 1991. Indeed, the desire of the then government to enact those authorisations without delay resulted in their being split off from the Bill and enacted separately, along with those parts of the Bill relating to the establishment, functions, and powers of the Privacy Commissioner. They were enacted as the Privacy Commissioner Act 1991, and later subsumed into the Privacy Act 1993.

9.9 The first Privacy Commissioner, Bruce Slane, commented that:[612]

> the Privacy Act 1993 fulfils a function of legitimising information matching. In my view, it is an appropriate function of data protection legislation to legitimise data matching if it avoids the ad hoc and uncontrolled application of the technique and subjects the activity to a satisfactory set of controls embodying fair information practices.

He considered that Part 10 of the Act and the information matching rules "are the key safeguards to ensure authorised information matching programmes are carried out fairly and successfully and in a way that protects the interests of affected individuals."[613]

9.10 There are both policy and technical issues relating to the use of information matching. The Privacy Commissioner has listed perceived negative impacts of information matching, including: [614]

- using information obtained for one purpose for an unrelated purpose;
- providing opportunities for "fishing" in government records with the hope of finding wrong-doing;
- initiating investigations without a pre-existing "cause to suspect";
- presuming people guilty simply because they are listed in a computer file, requiring them to prove their innocence;
- multiplying the effects on individuals of errors in government databases;
- undermining trust by dispersing information obtained by one agency in confidence;
- disclosing an individual's data without the individual's knowledge;
- taking action against individuals based on incorrect information or incorrect matching;
- taking action against individuals without their knowledge; and
- removing common sense and human judgment if decisions are automated.[615]

612 Office of the Privacy Commissioner *Review of Statutory Authorities for Information Matching* (Wellington, 1999) para 3.2.1.

613 Office of the Privacy Commissioner *Amendment of Information Matching rules* (Wellington, 2001) para 2.2.

614 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 39; Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 41.

615 For an excellent discussion of the issues relating to automated decision-making and due process, see Danielle Citron "Technological Due Process" (2008) 85 Wash U L Rev 1249.

9.11 From a technical point of view, a simplistic view of information matching as merely comparing one set of data against another belies a number of serious issues. These are well summarised in the Privacy Commissioner's 2008 Annual Report:[616]

> On the surface, using a computer to compare one set of records with another seems straightforward. However, this is rarely the case. For a start, the matching is usually against another organisation's information, which may mean a host of differences from a technical perspective as well as from organisational legal and even social perspectives. The two sets of data that are compared are likely to have been collected for different purposes, in different contexts and at different times, and may have different levels of detail, accuracy or format. For example, one data set may only contain the year of birth rather than the full date of birth, or may only contain informal preferred first names (aliases) rather than the full first names as listed on a passport. Seemingly objective characteristics such as address and declared income can differ on two databases for a variety of reasons, many of which do not indicate an intention to deceive anyone.
>
> Through the process of comparing records from different sources, information matching seeks to discover new facts about an individual by inferring that two records relate to the same person. For example, finding that an individual on the list of beneficiaries appears to be the same individual shown on another department's list of travellers departing overseas, suggests that a beneficiary has travelled overseas. However, all that matching actually delivers is an inference that these records are likely to belong to the same person; the match alone cannot deliver certainty about this. Mismatches can arise from incomplete, inaccurate or simply similar data.

9.12 Information matching involves the transfer of vast amounts of personal information from one agency to another. This raises the risk of accidental or deliberate loss or disclosure of the data. Under the Privacy Act, online matching is not permitted unless the approval of the Privacy Commissioner is obtained, and conditions may be imposed on such approvals to safeguard the data involved. The 2009 Annual Report of the Privacy Commissioner reports that, as at 30 June 2009, online transfer was used in 26 of the 50 active data matching programmes.[617] With respect to programmes where data is physically transferred between agencies, the Privacy Commissioner has required that the data is encrypted to safeguard the security of the data if it is lost or stolen. The Privacy Commissioner reports that, as at 30 June 2009, 19 matching programmes involve physical transfer, and of those 19 programmes, only one still involves unencrypted information being transferred.[618]

616 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 39.

617 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 45.

618 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 44.

9.13 It is because of the risks to privacy, the risks of adverse action being taken against individuals without justification, and the risk of undermining public trust and confidence in government, that the Privacy Act imposes controls on information matching. These controls are directed at:[619]

- authorisation – making sure that only programmes clearly justified in the public interest are approved;
- operation – ensuring that programmes are operated consistently with fair information practices; and
- evaluation – subjecting programmes to periodic reviews and possible cancellation.

The basic framework

9.14 The Act controls information matching by providing:

- for its authorisation by statute (an "information matching provision" – these are set out in Schedule 3 of the Act);
- that information matching programmes carried out by agencies ("specified agencies", defined in section 97) must be done pursuant to information matching agreements that comply with certain rules; and
- that certain procedural safeguards must be followed before action ("adverse action", defined in section 97) is taken against an individual in reliance on the results of a matching programme.

9.15 If an information matching provision is in place authorising an information matching programme, the following requirements and safeguards apply:

- The specified agencies authorised to participate in the information matching programme must have in place an information matching agreement before they disclose or receive personal information for the purposes of the programme.[620]
- The information matching agreement must incorporate provisions that reflect the information matching rules set out in Schedule 4 of the Act, or provisions that are no less onerous.[621] The information matching rules are discussed below.
- The specified agencies must comply with the agreement,[622] and must supply a copy (and any subsequent amendments) to the Privacy Commissioner.[623]
- The agencies involved in an information matching programme must take all reasonable steps to ensure that individuals who will be affected by the programme are notified of it, unless to do so would be likely to frustrate the objective of the programme.[624]
- If an information matching programme produces a "discrepancy",[625] the agency must, within 60 working days, make a decision whether or not to take adverse action against an individual on the basis of that discrepancy. If no

619 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 40.

620 Privacy Act 1993, s 99(1).

621 Privacy Act 1993, s 99(2).

622 Privacy Act 1993, s 99(2).

623 Privacy Act 1993, s 99(4).

624 Privacy Act 1993, sch 4, r 1.

625 A discrepancy (defined in section 97) "in relation to an authorised information matching programme, means a result of that programme that warrants the taking of further action by any agency for the purpose of giving effect to the objective of the programme."

decision to take adverse action is made within that period, the agency must destroy the information that disclosed the discrepancy.[626]

- The adverse action must be commenced within 12 months of obtaining the information that disclosed the discrepancy.[627]

9.16 Before an agency takes adverse action against an individual on the basis of a discrepancy, the agency must:

- notify the individual, in writing, of the particulars of the discrepancy and of the adverse action that it proposes to take;[628]
- tell the individual that he or she has five working days from receiving the notice to provide a good reason why the adverse action should not be taken;[629] and
- wait for those five working days to expire.[630]

In some cases, an agency can take adverse action against an individual without complying with the notice and delay requirements in section 103(1). There is a general exemption if compliance would prejudice any investigation into the commission of an offence or the possible commission of an offence.[631] In addition, there are specific exemptions for certain agencies in respect of certain information matching programmes.[632]

9.17 An agency to which personal information is disclosed for use in an information matching programme cannot keep the information indefinitely. If the information does not reveal a discrepancy, the agency must destroy that information as soon as practicable.[633] If the information reveals a discrepancy, the agency must destroy that information as soon as practicable after the information is no longer needed for the purposes of taking any adverse action against any individual.[634]

9.18 Likewise, an agency that holds information produced by an information matching programme cannot keep the information indefinitely. The agency must destroy the information:

- if the agency becomes aware of a discrepancy as a result of the information, and the agency has not made a decision to take adverse action against any individual on the basis of the discrepancy within 60 working days of becoming aware of the discrepancy;[635] or
- as soon as practicable after the agency decides not to take adverse action against any individual on the basis of the information;[636] or
- as soon as practicable after the information is no longer needed for the purposes of taking adverse action against any individual.[637]

---

626 Privacy Act 1993, s 101(1).
627 Privacy Act 1993, s 101(2).
628 Privacy Act 1993, s 103(1)(a)(i).
629 Privacy Act 1993, s 103(1)(a)(ii).
630 Privacy Act 1993, s 103(1)(a)(ii).
631 Privacy Act 1993, s 103(2).
632 Privacy Act 1993, ss 103(1A), (1B), (2A); Corrections Act 2004, s 180C.
633 Privacy Act 1993, sch 4, r 6(1).
634 Privacy Act 1993, sch 4, r 6(2).
635 Privacy Act 1993, s 101(1).
636 Privacy Act 1993, s 101(3).
637 Privacy Act 1993, s 101(4).

9.19 The Inland Revenue Department (IRD) is exempt from the requirements in section 101 and rule 6. We comment on the justification for this exemption later in the chapter.

9.20 The Privacy Commissioner can extend the time limit set out in section 101 in respect of information produced by an information matching programme if satisfied that an agency cannot reasonably be required to meet it, for example because of the amount of the information or the complexity of the issues involved.[638]

9.21 A failure to comply with the provisions of Part 10 in relation to an individual is an action that is an interference with the privacy of that individual,[639] and can therefore be the subject of a complaint to the Privacy Commissioner under section 67.

9.22 The Act imposes a number of detailed reporting requirements with respect to information matching programmes, as follows:

- Whenever required by the Privacy Commissioner, the agencies involved in a programme must provide the Commissioner with a report setting out whatever details the Commissioner requires.[640]
- The Privacy Commissioner's annual report must include a report on each information matching programme carried out during the year to which the annual report relates.[641]

9.23 The Act also provides for authorised information matching programmes to be subject to periodic evaluation.[642] The Privacy Commissioner is required to review the operation of every information matching provision at intervals of not more than five years, consider whether or not the authority conferred by the provision should be continued or whether any amendments to the provision are necessary or desirable, and report his or her findings to the responsible Minister.[643]

9.24 The Privacy Commissioner also has a function of examining and reporting on proposed legislation where the Commissioner considers that personal information authorised to be collected or disclosed by a public sector agency under the proposed legislation might be used for the purpose of an information matching programme.[644] In the course of that examination, the Commissioner is to have particular regard to the matters set out in section 98.

9.25 A special information matching regime is provided for under the Social Welfare (Transitional Provisions) Act 1990. This provides for the exchange of information between New Zealand and other countries under reciprocal social security agreements or conventions. The special regime is examined in more detail below.

638 Privacy Act 1993, s 102.

639 Privacy Act 1993, s 66(1)(a)(iii).

640 Privacy Act 1993, s 104.

641 Privacy Act 1993, s 105.

642 Privacy Act 1993, s 106.

643 Privacy Act 1993, s 106.

644 Privacy Act 1993, s 13(1)(f).

The information matching rules in Schedule 4

9.26 The information matching rules are set out in Schedule 4 of the Act. They are based to a large extent on the provisions of the Australian federal Data-matching Program (Assistance and Tax) Act 1990.[645]

9.27 The information matching rules are a mixture of general and detailed technical requirements. The key provisions of the information matching rules are as follows:

- Agencies involved in an information matching programme must take all reasonable steps to ensure that individuals who will be affected by the programme are notified of it, unless that would be likely to frustrate the objective of the programme (*rule 1*).
- Unique identifiers cannot be used as part of an information matching programme, unless their use is essential in the success of the programme (*rule 2*).
- Online computer connections must not be used to transfer information between agencies for the purposes of an information matching programme, unless the Privacy Commissioner approves the transfer (*rule 3*).
- The agency primarily responsible for the operation of an information matching programme must establish and maintain detailed technical standards governing the operation of the programme. These standards must deal with certain matters set out in the rules (such as how the integrity of the information to be used in the programme, and the integrity of the programme itself, are to be maintained, and the security features included within the programme), and be incorporated in a Technical Standards Report. Compliance with the requirements set out in a Technical Standards Report is mandatory for all agencies involved in the relevant information matching programme (*rule 4*).
- Agencies involved in information matching programmes must have reasonable procedures for confirming the validity of discrepancies before seeking to rely on them as the basis for action in respect of an individual, unless there are reasonable grounds to believe that the results are unlikely to be in error (*rule 5*).
- Personal information disclosed for use in an information matching programme and that does not reveal a discrepancy must be destroyed as soon as practicable, and personal information that does reveal a discrepancy must be destroyed as soon as practicable after it is no longer needed for the purposes of taking any adverse action (*rule 6*).
- Information used in information matching programmes must not be linked or merged to create a new separate register or databank of information about the individuals to whom the information relates (*rule 7*).
- Yearly limits on the number of times matching is carried out under a programme must be established for programmes that are to last longer than a year or indefinitely (*rule 8*).

645 This Act is examined in more detail below at paragraphs 9.73–9.75.

9.28 Section 107 of the Privacy Act authorises the amendment of the information matching rules by Order in Council. Amendments cannot be made otherwise than in accordance with recommendations of the Privacy Commissioner. Section 107 states that amendments can be made for the purposes of Part 10, but there is no other statement of the scope of section 107.

9.29 The power in section 107 has never been exercised. However, the Privacy Commissioner issued special reports in 2001[646] and 2003[647] recommending replacement of the information matching rules. These recommendations followed on from and built on the Commissioner's recommendations in *Necessary and Desirable*.

Information matching programmes

9.30 The 2009 Annual Report of the Privacy Commissioner indicates that there are currently 50 active information matching programmes in place,[648] up from 46 in 2008.[649] In the 2008/2009 reporting year the Office of the Privacy Commissioner provided assistance on or commented on one new authorisation, the start of six new matches, and numerous changes to the scope and conditions of existing agreements.[650] During the same period, Parliament passed five new matching authorisations, all of which involved amendments to the Births, Deaths, Marriages and Relationships Registration Act 1995.[651]

9.31 The Passport Eligibility Programme authorised by section 78A of the Births, Deaths, Marriages, and Relationships Registration Act 1995 is a simple example of an information matching programme. The purpose of the programme is to assist in determining whether or not a person is eligible for a New Zealand passport, and to detect fraudulent applications. Identity information on passport applications is matched against births, deaths, and marriages registers. A match with an entry in the births and marriages registers means that the processing of the application can continue. A match with an entry on the deaths register halts the processing of the application so that a possible case of fraud can be investigated.[652]

646 Office of the Privacy Commissioner *Amendment of Information Matching rules. Report by the Privacy Commissioner to the Minister of Justice recommending that making of an Order in Council to revoke the Fourth Schedule to Privacy Act 1993 and to substitute a new Schedule containing a revised set of information matching rules* (Wellington, June 2001).

647 Office of the Privacy Commissioner *Amendment of Information Matching Rules: supplementary report. Report by the Privacy Commissioner to the Minister of Justice making supplementary recommendations to those contained in a report of 28 June 2001 recommending the replacement of the information matching rules by Order in Council* (Wellington, August 2003).

648 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 42.

649 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 46.

650 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 42.

651 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 42.

652 For more on this programme see Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 50.

Matching that is outside Part 10

9.32 Part 10 does not control all information matching. To the extent that particular information matching would not otherwise be permitted by the privacy principles, an information matching provision specified in Schedule 3 provides the authority to undertake information matching in compliance with Part 10.

9.33 Section 108 provides that, where the collection or disclosure of information is authorised by an information matching provision, the maintenance of the law exceptions in privacy principles 2 and 11 cannot be used to avoid the controls on information matching in the Act. Equally, section 109 provides that agencies cannot use the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987 to exchange information and thereby avoid the controls on information matching.[653]

9.34 However, except where sections 108 and 109 apply, Part 10 does not apply where an agency is able to carry out information matching without reliance on the authority of an information matching provision. The Privacy Commissioner, in *Necessary and Desirable*, identified situations where this might be possible:[654]

- if the matching is authorised, either generally or specifically, by a statutory provision that is not listed as an information matching provision in Schedule 3;
- if the matching is able to be carried out consistently with the privacy principles; or
- if the matching is authorised by the Privacy Commissioner under section 54 of the Act, or by a code of practice.

9.35 The limited application of section 108 also raises the possibility that, even though an information matching provision is specified in Schedule 3, an agency could collect, disclose, and use personal information for the purposes of a matching programme in compliance with the privacy principles without relying on the maintenance of the law exception to principles 2 and 11. The agency would then effectively have a choice as to whether it complied with Part 10 or not.[655] Later in this chapter we explain our dissatisfaction with this position.

INFORMATION MATCHING UNDER THE SOCIAL WELFARE (TRANSITIONAL PROVISIONS) ACT 1990

9.36 Sections 19 to 19D of the Social Welfare (Transitional Provisions) Act 1990 enact a framework under which legal effect in New Zealand can be given to agreements or conventions between the New Zealand Government and the governments of other countries providing for mutual assistance in recovering social security debts and supplying information for social security purposes. Legal effect is given to an agreement by the making of an Order in Council that declares that certain provisions of the agreement or convention have the force of law in New Zealand, and that certain New Zealand enactments (such as the Social Security Act 1964) have effect subject to such modifications as may be required for the purpose of giving effect to the agreement or convention.

653 Privacy Act 1993, s 109.

654 See *Necessary and Desirable,* para 10.1.14.

655 For a discussion of the "choice of power" situation and the legal principles that might apply, see further Christopher Enright *Federal Administrative Law* (Federation Press, Sydney, 2001) 83.

9.37 The Act sets out certain preconditions that must be complied with before an Order in Council can be made. If an agreement or convention contains provision for mutual assistance between the parties in the recovery of social security debts or for the supply of information, an Order in Council cannot be made unless the Privacy Commissioner has first reported to the Minister responsible for the administration of the Act and the Minister of Justice.[656] The report must consider whether or not the provision in the agreement or convention complies with the privacy principles (having regard to the information matching guidelines set out in section 98 of the Privacy Act),[657] and if the provision provides for the exchange of information between the parties, the adequacy of the other country's privacy protection for personal information that may be supplied by New Zealand.[658]

9.38 A provision in an agreement or convention providing for the exchange of information must be subject to a number of terms and conditions set out in section 19C of the Social Welfare (Transitional Provisions) Act, or terms and conditions to the same effect. Those terms and conditions include a requirement that any exchange of personal information be made only for social security purposes (although information supplied may be passed on to taxation authorities for tax assessment and enforcement purposes).[659] Any exchange of information must be made in accordance with an agreement between the relevant organisations in each country,[660] and, in relation to New Zealand, the agreement must be approved by the Privacy Commissioner,[661] contain the safeguards that must be included in an information matching agreement under the Privacy Act,[662] and require the information matching rules to be applied.[663] Information supplied to a country under the agreement or convention must also be subject to the same privacy protections as other personal information obtained under that country's social security laws.[664]

9.39 If information is supplied to the relevant New Zealand authority under a provision of an agreement or convention, section 19D(3) of the Act imposes procedural requirements that are similar to those in section 103 of the Privacy Act before the information can used to take action against an individual. In addition, sections 100 to 102 and 104 to 106 of the Privacy Act apply in respect of the provision as if the provision were an authorised information matching programme. The oversight and reporting functions of the Privacy Commissioner therefore apply to the activities carried out under the provision.

---

656 Social Welfare (Transitional Provisions) Act 1990, s 19(2A). See, for example, Office of the Privacy Commissioner *Exchange of Social Security Information with the Netherlands: Report by the Privacy Commissioner to the Minister of Justice and the Minister of Social Development and Employment pursuant to section 19(2A) of the Social Welfare (Transitional Provisions) Act 1990 in relation to mutual assistance provisions in the revised reciprocity agreement on social security between New Zealand and the Netherlands* (Wellington, 2003). Available at www.privacy.org.nz/exchange-of-social-security-information-with-the-netherlands.

657 Social Welfare (Transitional Provisions) Act 1990, s 19(2A)(a).

658 Social Welfare (Transitional Provisions) Act 1990, s 19(2A)(b).

659 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(a).

660 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d).

661 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d)(v).

662 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d)(iii).

663 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d)(iv).

664 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(e).

9.40 Six active information matching programmes are currently carried out under two separate reciprocity agreements in place under section 19 of the Social Welfare (Transitional Provisions) Act 1990. Two programmes operate under an agreement between New Zealand and Australia, and four operate under an agreement between New Zealand and the Netherlands.[665] The operation of all six active information matching programmes is audited each year by the Privacy Commissioner. The 2009 Annual Report of the Privacy Commissioner indicates satisfaction that the programmes were generally conducted in accordance with applicable statutory requirements.[666]

OVERSIGHT OF INFORMATION MATCHING PROGRAMMES BY THE PRIVACY COMMISSIONER

Levels of oversight

9.41 The Privacy Commissioner performs an oversight role in relation to information matching at three levels. First, the Commissioner considers and reports on new proposals to authorise information matching under sections 13(1)(f) and 98 of the Privacy Act 1993 and section 19A of the Social Welfare (Transitional Provisions) Act 1990. Secondly, the Commissioner monitors and reports on authorised information matching programmes in accordance with Part 10 of the Privacy Act 1993 (including where this Part is applied by section 19D(3)(e) of the Social Welfare (Transitional Provisions) Act 1990). Thirdly, the Commissioner is required to undertake periodic reviews of the statutory authorities for information matching under section 106.

Reporting on proposed authorisations for information matching

9.42 The first function of considering and reporting on proposed information matching authorisations requires little comment. The function is part of a wider governmental and legislative process that seeks to ensure that new proposals to authorise information matching are justifiable, well scoped, and well designed. In *Necessary and Desirable*, the Privacy Commissioner found the process to be working satisfactorily, and made a small number of recommendations for minor improvements.[667] These related to the information matching guidelines set out in section 98 of the Privacy Act.

9.43 As part of the process of considering a legislative proposal for an information matching programme, the Privacy Commissioner requires the relevant agency to prepare an Information Matching Privacy Impact Assessment (IMPIA) report, describing the programme and its objectives, and how it will comply with the Privacy Act 1993. A detailed analysis of the proposal against the information matching guidelines set out in section 98 of the Privacy Act is a key part of the IMPIA. A guidance note for agencies seeking legislative provision for information matching has been prepared by the Privacy Commissioner and is available on the Privacy Commissioner's website.[668]

665 See "Data Matching – Operating Programmes" www.privacy.org.nz/operating-programmes (accessed 15 February 2010).

666 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, November 2009) 69, 77–79.

667 *Necessary and Desirable,* recommendations 122–124.

668 Office of the Privacy Commissioner *Guidance Note for Departments Seeking Legislative Provision for Information Matching* (Wellington, 2008). Available online at www.privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching.

9.44 We discuss below the suggestion that this process be further enhanced by imposing a legislative requirement for agencies to prepare a written assessment of a proposed information matching programme in the form of a "programme protocol".[669]

Monitoring and reporting on information matching programmes

9.45 The monitoring and reporting functions of the Privacy Commissioner in relation to information matching programmes constitute a major activity for the Commissioner and her staff. Section 105 of the Privacy Act requires that the Commissioner report each year on the information matching programmes carried out during that year, and include an assessment of the extent of each programme's compliance with sections 99 to 103 of the Act and the information matching rules. The work involves a significant resource commitment on the part of the Commissioner. Two fulltime resources within what is a small office are devoted to information matching. The 2009 Annual Report of the Commissioner reports on 50 programmes, and this constitutes close to a third of the Commissioner's report.

9.46 The Privacy Commissioner's oversight of an information matching programme does result in the identification of issues that the relevant agency needs to address. The Commissioner's 2009 Annual Report indicates that all but one[670] of the 50 operative programmes were generally operated in compliance with the Privacy Act (and, where applicable, the Social Welfare (Transitional Provisions) Act 1990), although in two cases she identified technical issues with programmes,[671] and in one other case identified issues with the agencies' retention and verification practices.[672] In her 2007 Annual Report, the Privacy Commissioner raised concerns about the quality of the matching results being acted upon in the Customs/Justice Fines Defaulters Alert Match, and indicated that on the basis of those concerns she could not confirm that the programme was being conducted in compliance with the Act.[673] As a result of those concerns, an inter-agency project team was established to review of the operation of this match (in conjunction with the Office of the Privacy Commissioner). The Commissioner's 2008 Annual Report indicated satisfaction with the operation of the programme, while noting that the review had highlighted a number of procedural arrangements that could be improved and that were in the process of being implemented.[674] The 2009 Annual Report shows that this matching programme is compliant with the requirements under the Act.[675]

669 See below paragraphs 9.128–9.131.

670 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2009) 65.

671 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 58, 63.

672 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 64–65.

673 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2007* (Wellington, 2007) 95.

674 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 107–108.

675 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 60.

Review of information matching authorities

9.47 The third function of the Privacy Commissioner in relation to information matching is to review the statutory authorities for information matching at intervals of not more than five years in accordance with section 106 of the Privacy Act. In carrying out a review, the Commissioner must consider whether or not the authority should be continued, and whether any amendments to the relevant statutory provision are necessary or desirable, and report his or her findings to the responsible Minister.

9.48 The Privacy Commissioner has published the results of two reviews carried out under section 106.[676] The first was published in May 1999, and reviewed authorities to carry out two information matching programmes under the Customs and Excise Act 1996 and the Tax Administration Act 1994. The second was published in May 2002, and reviewed authorities to carry out four information matching programmes under the Penal Institutions Act 1954, the Tax Administration Act 1994, and the Immigration Act 1987. Section 106 of the Privacy Act does not prescribe the considerations that the Commissioner should take into account in undertaking a review, but the Commissioner indicated in both reviews that the information matching guidelines set out in section 98 of the Act are a major basis of that consideration.

9.49 Of the six authorities for information matching reviewed by the Privacy Commissioner, the Commissioner has recommended that five be continued and one be repealed (the NZIS/MSD Immigration match under the Immigration Act 1987, on the basis that the authority was not being utilised).[677] In relation to one authority, the Commissioner recommended the repeal of a related provision of the Privacy Act (section 103(1A)).[678] None of these recommendations have been implemented. There is no requirement in section 106 of the Privacy Act for the Government to respond to any recommendations in a Commissioner's report under that section.

9.50 No further reports on section 106 reviews have been published. The 2004 Annual Report of the Privacy Commissioner indicated that the objective of completing section 106 reviews of a further three information matching programmes had not been achieved due to demands on limited resources.[679] The 2008 Annual Report of the Privacy Commissioner indicated that the Commissioner is currently carrying out a section 106 review of one of the information matching programmes carried out under section 84 of the Tax Administration Act 1994, but no timeframe was outlined.[680] At the date of writing, this review has not been finalised.

---

676 Both are available online at www.privacy.org.nz/information-matching-reports-and-reviews.

677 Office of the Privacy Commissioner *Review of statutory authorities for information matching (Second Report)* (Wellington, May 2002) 31.

678 Office of the Privacy Commissioner *Review of statutory authorities for information matching* (Wellington, May 1999) 7.

679 Office of the Privacy Commissioner *Annual Report of the Privacy Commissioner for the year ended 30 June 2004* (Wellington, November 2004) 111.

680 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, November 2008) 92.

9.51 The review of authorising provisions for information matching is an important part of the overall system of oversight of information matching. Since these authorising provisions constitute an exception to the privacy principles, it is appropriate that each authority is regularly reviewed to establish whether or not it is still needed, whether or not the expected benefits from the programme are (still) being realised and are sufficient to justify the inroads into privacy that the programme involves, and whether or not the actual operation of the programme over the review period provides sufficient confidence that the risks to privacy arising from the programme have been sufficiently well-managed to justify the continued existence of the programme. Indeed, the section 106 review procedure was included in the Act, as an adjunct to the requirement that all information matching programmes be authorised by statute, in the place of the procedure originally proposed in the Privacy of Information Bill as introduced. Under that procedure, in addition to certain statutorily authorised information matching programmes, the Privacy Commissioner would have been empowered to issue both permanent and time-limited information matching approvals. The Commissioner would also have been empowered to revoke any such approval on the grounds that it no longer met the requirements for approval or for non-compliance with the conditions of the approval or the information matching rules.

9.52 Resourcing constraints have prevented both the current and the previous Privacy Commissioner from undertaking the regular reviews of information matching authorities required by section 106. We make some suggestions about this below.[681]

Report on an unauthorised information matching programme

9.53 There is one reported case of information matching not authorised by statute (that is, it had not been listed as an "authorised information matching programme" subject to Part 10 of the Act) being undertaken by a New Zealand government agency. In 2000, the Privacy Commissioner investigated information matching undertaken in 1998 by the Department for Courts.[682] The programme matched the Department's list of fines defaulters against personal details on the motor vehicle register in order to obtain updated address information.

9.54 Significant data quality problems with the programme meant that many of the people who were identified in the data match, and who were subsequently sent letters requiring them to repay fines promptly, were not the individuals who owed the fines. While the further particulars of the incident need not be considered here, in his report the then Privacy Commissioner stated:[683]

> I am extremely concerned about departments seeking to undertake data matching which has not been authorised through Part X of the Act. It is quite at variance with the Government policy lying behind the establishment of Part X. It makes little sense that Cabinet should authorise some public sector data matching subject to strict controls while officials take it upon themselves to initiate other significant matching totally

681 See paragraphs 9.138–9.141 below.

682 Office of the Privacy Commissioner *Unauthorised information matching between Department for Courts and motor vehicle register: Report to the Ministers of Justice, Courts and Transport in relation to an inquiry into events surrounding unauthorised information matching programme operated in mid-1998* (Wellington, 2000).

683 Office of the Privacy Commissioner *Unauthorised information matching between Department for Courts and motor vehicle register: Report to the Ministers of Justice, Courts and Transport in relation to an inquiry into events surrounding unauthorised information matching programme operated in mid-1998* (Wellington, 2000) 2.

unregulated by Part X. If public confidence is to be maintained in the fair handling of public sector information and in the responsible use of data matching, it is critical that departments go through the rigorous process of justification and assessment in establishing a programme and that the practice be authorised at the highest level.

Other activities

9.55 In addition to the three specific oversight functions conferred on the Privacy Commissioner by the Act, the Commissioner and her staff devote considerable resources towards informing and educating government agencies involved in information matching. The Commissioner holds meetings of agencies involved with or interested in information matching. Training workshops are held for people who are or may be involved in developing an authorised information matching programme. An Information Matching Bulletin containing information and articles on information matching is published periodically.[684] A *Guidance Note for Departments Seeking Legislative Provision for Information Matching* has been produced along with a resource document about the information matching guidelines,[685] and draft Guidance notes for online transfer approvals have also been distributed for feedback and comment.[686] In addition, for the last few years, an *Information Matching Compliance Auditing Information Pack* has been made available each year to agencies involved in information matching.[687] The pack provides the government agencies with audit templates and guidance material to enable them to provide the statutorily required reports to the Privacy Commissioner on their information matching programmes.

CHANGES IN INFORMATION MATCHING SINCE 1991

9.56 There have been significant changes in the extent and nature of information matching since the enactment of the original information matching controls in the Privacy Commissioner Act 1991. Societal, international, and technological changes have also had an impact. The following are the key changes in information matching since 1991:

- The number of agencies involved has grown significantly. In 1991, eight separate enactments provided 10 individual statutory authorisations[688] for information matching involving eight separate agencies. As at September 2009, 16 separate enactments provide over 40 individual statutory authorisations for information matching involving at least 24 separate agencies (including generic classes of agency such as institutions and private training establishments within the meaning of section 159 of the Education Act 1989). The Privacy Commissioner reports that, between 1998 and 2008, the number of agencies from which data for information matching programmes is sourced has doubled, and the number of agencies that use this source data has more than doubled.[689]
- The number of active information matching programmes has increased

684 Three editions were published during the 2008/2009 reporting year. Available online at www.privacy.org.nz/information-matching-bulletins.

685 Office of the Privacy Commissioner *Guidance Note for Departments Seeking Legislative Provision for Information Matching* (Wellington, May 2008).

686 Available online at www.privacy.org.nz/resources-for-government-agencies (accessed 13 January 2010).

687 Office of the Privacy Commissioner *Information Matching Compliance Auditing Information Pack* (Wellington, 2009).

688 These are the information matching provisions that were listed in Schedule 3 of the Privacy Commissioner Act 1991.

689 Office of the Privacy Commissioner *Information Matching Bulletin* (December 2008) 2.

significantly. The Privacy Commissioner reports that, between 1998 and 2008, the number increased from 12 to 46 (out of a total of 80 authorised information matching programmes).[690] This number increased to 50 in 2009.

- The purposes for which information matching is carried out have evolved, with a shift towards purposes that are more beneficial to individuals than the original focus on detecting and avoiding benefit fraud. The Privacy Commissioner has compared the purposes of the information matching programmes carried out in 1997/98 with those carried out in 2007/08. Over 75 per cent of the matching programmes carried out in 1997/98 were to confirm eligibility for a benefit or to detect illegal behaviour. In 2007/08, only just over 50 per cent of information matching programmes were carried out for those purposes. Purposes that had assumed greater significance included locating people, updating data, and identifying unclaimed entitlements.[691]
- A huge increase in the amount of personal information that is held in computerised form and massive advances in information technology have significantly increased the ability of agencies to undertake information matching. Not only does this increase the scale of information matching that is possible,[692] it is now also economic to undertake much smaller matches than previously. However, as information systems technology has evolved, concerns have been expressed that data quality problems have increased as well. One commentator has suggested that this is the result of rapid systems development that has made quality hard to control, and that standards, techniques, methods, and tools for managing quality have evolved at a slower pace than the systems they support.[693]
- Information matching was originally carried out through the transfer of data on computer tape or disk. The information matching rules prohibit online matching without the approval of the Privacy Commissioner. In *Necessary and Desirable*, the then Privacy Commissioner reported that he had granted such an approval in respect of one information matching programme. The Privacy Commissioner's 2009 Annual Report indicates that over half (26) of the 50 active programmes have approvals to undertake online matching.[694]
- The original information matching programmes involved data generated and matched domestically. Some information matching programmes now involve the transfer of data to another jurisdiction, or receipt of data from another jurisdiction. Social security mutual assistance schemes authorised under the Social Welfare (Transitional Provisions) Act 1990 are an example.
- The initial authorised information matching involved core government agencies such as the Department of Social Welfare and the IRD. A broader range of

690 Office of the Privacy Commissioner *Information Matching Bulletin* (December 2008) 2.

691 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 46–47.

692 For example, in the year to 30 June 2007, the Department of Social Development's National Data Match Centre compared more than 12 million records with other agencies. This resulted in 193,358 matches and 18,588 cases of overpayments. The total value of these overpayments was $19 million. See Office of the Auditor-General "Ministry of Social Development: Preventing, detecting, and investigating benefit fraud, performance audit report under section 16 of the Public Audit Act 2001" (Wellington, 2008) 31.

693 The commentator writes under the profile "Vijikumar" at http://dataqualityaccuracy.blogspot.com. See the articles "The Data Quality Problem", "Definition of Accurate Data", "Sources of Inaccurate Data", and "Implementing a Data Quality Assurance Program" published on that website on 13 December 2007. See also "Data quality accuracy dimension", a two-part article by Colin Trotter in the May and June 2008 *Information Matching Bulletins* published by the Office of the Privacy Commissioner, Wellington.

694 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 45.

government agencies are now involved in information matching, such as district health boards and the New Zealand Transport Agency. Private sector agencies now supply some of the information used in information matching, such as private training establishments under the Education Act 1989.

- Some of the procedural requirements imposed by Privacy Act as originally enacted have been overridden by subsequent legislative amendments for some information matching programmes. In five cases, the requirement in section 103 that people must be notified before adverse action is taken against them on the basis of the result of a match, and given an opportunity to challenge the proposed action, has been overridden.

9.57 Our overall conclusion from these developments is that the scale and importance of information matching in the operation of public sector agencies means that the controls and protections in the Privacy Act with respect to information matching are even more important now than when the Act was first enacted.

INFORMATION MATCHING AND DATA MINING

9.58 There is a close relationship between information matching and data mining. Indeed, information matching might be regarded as a specialised subset of data mining. Various definitions of data mining have been put forward. The Australian Law Reform Commission (ALRC) adopted a definition from the Ontario Information and Privacy Commissioner: "a set of automated techniques used to extract buried or previously unknown pieces of information from large databases".[695] A more expansive definition was proffered by the US Government Accountability Office (GAO) in a 2004 report on data mining by federal agencies: "the application of database technology and techniques – such as statistical analysis and modelling – to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results."[696]

9.59 From the description of information matching above, it can be seen that both data mining and information matching employ modern technology to analyse a vast amount of previously inaccessible and unconnected information and to provide personal information about an individual. Both do so with various degrees of accuracy.

9.60 While information matching tends to be associated with public sector agencies, data mining spans both public and private sectors. Organisations in the private sector use it for such purposes as market research, design of sales or marketing campaigns, product development, customer relationship management, financial analysis, and fraud detection.

695 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 9.51.

696 United States Government Accountability Office *Data Mining: Federal Efforts Cover a Wide Range of Uses. Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate* (GAO-04-548, Washington D.C., May 2004). See also Government Accountability Office *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain* (GAO-05-866, Washington D.C. August 2005).

9.61 The 2004 GAO report indicates that US Federal agencies use data mining for a variety of purposes, such as improving service or performance, detecting fraud, waste and abuse, analyzing scientific and research information, managing human resources, detecting criminal activities or patterns, analysing intelligence and detecting terrorist activities.[697]

9.62 Concerns about data mining are very similar to those about information matching. The ALRC summarised these as follows:[698]

- Data mining is carried out without the data subject's knowledge or consent, and can reveal large amounts of previously unknown personal information about that individual. As a consequence, informing the individual about the collection and use of the information is difficult, and it is difficult for the individual to seek access to the information.
- Data mining uses information collected for different purposes and in different contexts. The source information may have been inaccurate at the time of collection or may have become inaccurate subsequently. This raises doubts about the accuracy of the information derived from the data mining. The combination of information collected from different sources compounds the danger of inaccuracy.
- Large amounts of personal information are collected and stored for the purpose of data mining, raising concerns about the security of the information. Note, however, that data mining can now be carried out without aggregating or homogenising the source information, which can be mined in many locations and in many formats.

9.63 The GAO has raised an additional concern about data mining: *function creep*.[699] The aggregation and organisation of large quantities of previously isolated pieces of information could tempt agencies to use the information for purposes beyond the scope originally specified when the information was collected.

9.64 Another US organisation, the Information Security and Privacy Advisory Board, produced a report in May 2009 recommending ways in which privacy law and policy might be updated in the light of technological change. It had this to say about data mining:[700]

> Data mining techniques represent a fundamental change in the way the government accesses and uses data. In the past, the government collected and processed data on one person at a time [that is, with particularity], either in the course of administering a government program or where there was some suspicion that a person was engaged in fraud, criminal conduct, terrorism or intelligence activity. The government was authorised to keep this data for long periods of time, and to retrieve, share and analyse it for compatible purposes without serious controls. New techniques like data mining undermine these protections as the government analyses information en masse.

697 United States Government Accountability Office *Data Mining: Federal Efforts Cover a Wide Range of Uses. Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate* (GAO-04-548, Washington D.C., May 2004) ii.

698 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) paras 9.53–9.54.

699 United States Government Accountability Office *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks. Report to the Chairman, Committee on Appropriations, House of Representatives (*GAO-07-293, Washington D.C., February 2007) 19.

700 Information Security and Privacy Advisory Board *Toward A 21st Century Framework for Federal Government Privacy Policy* (Washington D.C., May 2009) 28.

9.65 In 2007 a Bill, the Federal Agency Data Mining Reporting Act 2007, was introduced into Congress.[701] It would not have imposed restrictions on data mining, but would have required the head of each department or agency of the Federal Government that engaged in any activity to use or develop data mining to submit an annual report to Congress on those activities. Data mining would have had a limited scope under the Act, essentially covering a programme involving pattern-based queries, searches, or other analyses of one or more electronic databases to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity. Excluded from the definition of "database" were telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources.

9.66 The ALRC made no specific recommendations relating to data mining, although the scope of their recommended Unified Privacy Principles relating to collection, notification, data quality, use, and disclosure would clearly impose limitations on the activity.

9.67 A relatively recent phenomenon is the huge growth in the use of the internet for social interaction, and the willingness of people to post personal (and often very sensitive) information about themselves (and others) on social networking and other websites.[702] Whether through ignorance or choice, users often place no or very few limits on access to this information by others. This means that a rich vein of personal information is now available to be mined by both the public and private sectors. The technological capability to extract the personal information is matched only by the willingness of people to disclose it. A recent newspaper article on government monitoring of social networking websites reports the case of a woman convicted of social welfare fraud for claiming a benefit when she was in a relationship.[703] Her Facebook and Bebo profiles stated that she was living in a relationship with the father of her child, when she had told welfare authorities that she was single. The article indicates that a number of other New Zealand government agencies are using social networking websites as sources of information.[704]

9.68 To the extent that data mining is not information matching, the collection, disclosure, use, and unique identifier restrictions in the Privacy Act, and any specific authorising legislation, apply. The Privacy Act has specifically dealt with information matching by government agencies from the outset because of the particular privacy issues that it raises. Given that data mining raises similar issues, and the enormous scope for its use (and misuse) in relation to the vast amount of personal information now available online, it may now be time to consider greater controls.

---

701 Pub L 110-53, 121 Stat 266, s 804 (2007). The Bill never became law, as it lapsed at the end of the Congressional session.

702 For more on social networking see chapter 13.

703 "Big Brother Watching our Lives Online" (4 April 2009) *Dominion Post* A10–11.

704 See also "Brits Consider Tracking All UK Facebook Traffic" (18 March 2009) http://news.zdnet.com (accessed 15 February 2010). This article reported that the UK government was considering the surveillance and retention of all communications on social networking sites. The UK government subsequently dropped the idea: see *Home Office Protecting the Public in a Changing Communications Environment* (April 2009).

9.69 In a 2004 report for the State Services Commission on citizens' responses to E-government, the researchers noted that there was a widespread belief among participants in the survey that government will not misuse information they provide via the internet – whether that information relates to their work or personal lives.[705] However they also noted that:[706]

> Confidence would be eroded if they found out that the government cross-matched data or extensively engaged in data mining—sharing data among departments and agencies and culling information from assorted databases to learn more about the public.

9.70 One possible starting point might be to require greater transparency and openness about data mining in New Zealand. A requirement on public agencies to report on their data mining activities, along the lines of the US legislation, is one option. We have an open mind on the issue. Public feedback on the level of concern about data mining, and how any concerns might be addressed, would be particularly valuable.

Q104 Should there be greater openness about data mining by public agencies? For example, should public agencies be required to report annually on their data mining activities?

OVERSEAS APPROACHES TO INFORMATION MATCHING

9.71 In this section we examine the information matching regimes in Australia, Canada, the United Kingdom, the USA, and Hong Kong to see if they offer any insights or lessons for New Zealand.

Australia

Federal

9.72 The Privacy Act 1988 (Cth) does not specifically regulate data matching, except in relation to the use of a tax-file number, but some of the Act's Privacy Principles may apply to the activity. National Privacy Principle 7.1, for instance, regulates the adoption and use by non-government entities of identifiers assigned by government entities.

9.73 The Data-matching Program (Assistance and Tax) Act 1990 provides authority for the transfer and matching of personal information between the Australian Taxation Office and certain other agencies. The provisions in Part 10 and Schedule 4 of the New Zealand Privacy Act were based closely on that Act. The purpose is to detect the overpayment of certain benefits, persons receiving duplicate benefits, and non-compliance with tax law obligations, as well as identifying people who are entitled to a benefit but not claiming it.

705 Rowena Cullen and Peter Hernon *Wired for Well-Being: Citizens' Response to e-government: A report presented to the E-government Unit, State Services Commission* (Wellington, 2004).

706 Rowena Cullen and Peter Hernon *Wired for Well-Being: Citizens' Response to e-government: A report presented to the E-government Unit, State Services Commission* (Wellington, 2004) 50.

9.74 The Act provides that agencies carrying out matching under the Act must comply with guidelines.[707] The latest guidelines issued by the Privacy Commissioner came into effect in 1997.

9.75 The effect of the Act and the guidelines is to set out what personal information can be used in data matching programmes, how data matching programmes are to be conducted, and how the results of a programme can be used. Procedural safeguards very similar to those applying under the New Zealand Act require individuals to be given a chance to dispute or explain the results of a matching programme before action is taken against them.

9.76 To provide guidance to agencies that carry out data-matching that is not covered by the 1990 Act, the Privacy Commissioner has issued voluntary data-matching guidelines.[708] Their aim is to ensure that data-matching programmes are designed and conducted in accordance with sound privacy practices and in a privacy-sensitive way.

9.77 The Guidelines also state that they aim to encourage a higher standard of regard for people's privacy rights in relation to data-matching than is required by bare compliance with the Information Privacy Principles.[709] In assessing compliance with the Information Privacy Principles, the Privacy Commissioner may take the guidelines into consideration, but non-adherence to the guidelines would not necessarily put an agency in breach of the Privacy Principles.

9.78 The ALRC considered suggestions that the voluntary data-matching guidelines applying to governmental agencies should be made mandatory, but rejected this on the basis that there is no indication that agencies are not currently complying with those guidelines.[710] It suggested that the Office of the Privacy Commissioner might review the adequacy of, and compliance with, the current guidelines if the Office considered this necessary.

Victoria

9.79 We note that a different approach to the regulation of data matching in Australia is favoured by the Office of the Victorian Privacy Commissioner.[711] That Office undertook an audit of data-matching activities in state and local government in Victoria in 2005. In its report, the Office stated its attraction to the New Zealand generic statute model for regulating data matching, as combining openness, precision, and oversight.[712]

---

707 Data Matching Program (Assistance and Tax) Act 1990 (Cth), s 12.

708 Office of the Privacy Commissioner (Cth) *The use of data matching in Commonwealth administration – Guidelines* (Sydney, February 1998).

709 Office of the Privacy Commissioner (Cth) *The use of data matching in Commonwealth administration – Guidelines* (Sydney, February 1998) 3.

710 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, Wellington) para 10.97.

711 Office of the Victorian Privacy Commissioner *Victorian Public Sector Data Matching Audit* (Melbourne, 2005).

712 Office of the Victorian Privacy Commissioner *Victorian Public Sector Data Matching Audit* (Melbourne, 2005) 1.

9.80 In its submission to the ALRC review, the Office of the Victorian Privacy Commissioner reported its preference for a generic statutory regime.[713] In the absence of such a statute the Victorian OPC recently published a guide on data matching for the Victorian public sector.[714]

Canada

9.81 In Canada, at the Federal level, the ability of agencies to collect, use, and disclose personal information for data matching purposes is generally governed by the requirements of the Privacy Act. At the detailed level, data matching is governed by a Treasury Board of Canada Secretariat Policy on Data Matching, published in 1989.[715] As a policy directive, it does not have the force of law. The policy requires that Federal agencies undertake a preliminary assessment of the feasibility of the proposed matching programme (including a cost-benefit analysis), and provide this assessment to the Privacy Commissioner at least 60 days before the programme begins to allow for an external review before it is implemented.

9.82 In a 2006 review of the Canadian Federal Privacy Act, the Canadian Privacy Commissioner reported that very few data matching proposals are reported to the Privacy Commissioner, and that the data matching policy was not well-known among agencies.[716] The Commissioner further indicated that data matching had long been a concern to that office, and that the Privacy Act lacked effective audit and control mechanisms on data matching.[717] Even though the Treasury Board data matching policy was to be revised, the Commissioner considered that legislative controls were required.[718]

United Kingdom

9.83 The Data Protection Act 1998 applies generally to information matching in both the public and private sectors in the United Kingdom, but contains no specific provisions regulating it. The ability of agencies to undertake information matching therefore depends on whether or not this will comply with the Act's data protection principles and other requirements. Compliance tends to be subsumed under the question of whether or not the information required for the matching can legally be shared by the agencies involved. This involves, amongst other things, assessing whether the information sharing is necessary, whether the information to be shared is relevant and not excessive, and whether the information will be processed fairly. The Information Commissioner has also issued an Information Sharing Framework Code of Practice.[719]

---

713 Office of the Victorian Privacy Commissioner *Submission to the Australian Law Reform Commission's Review of Australian Privacy Law (*Melbourne, December 2007).

714 Office of the Victorian Privacy Commissioner *Data Matching in the Public Interest: A guide for the Victorian public sector (*Melbourne, 2009).

715 Treasury Board Secretariat *Policy on Data Matching* (1989), available online at www.tbs-sct.gc.ca (accessed 15 February 2010).

716 Office of the Privacy Commissioner of Canada *Government Accountability for Personal Information: Reforming the Privacy Act* (Ottawa, 2006).

717 Office of the Privacy Commissioner of Canada *Government Accountability for Personal Information: Reforming the Privacy Act* (Ottawa, 2006).

718 Office of the Privacy Commissioner of Canada *Government Accountability for Personal Information: Reforming the Privacy Act* (Ottawa, June 2006).

719 Information Commissioner's Office *Framework Code of Practice for Sharing Personal Information* (London, 2007).

In addition, there are some specific legislative authorities for information matching in the UK. For example, the UK Audit Commission has powers under Part 2A of the Audit Commission Act 1998 to undertake data matching for the purpose of assisting in the prevention and detection of fraud.

United States

9.84 The Office of Management and Budget (OMB) issued guidelines in 1979 in relation to computer matching at the Federal level. The guidelines were revised and reissued in 1982. The guidelines allowed computer matching to be undertaken under the "routine use" exemption to the Privacy Act 1974, and imposed controls such as a requirement for prior notification of a matching programme in the Federal Register setting out the benefits, costs, potential harm, and alternatives. Agencies were also to report on the match to the Director of the OMB, Speaker of the House, and President of the Senate. The guideline approach was not, however, a success. One commentator, Priscilla Regan, observes that "agencies did not follow the guidelines, the OMB did not monitor agencies' activities, the public and interest groups did not respond to *Federal Register* notices, and there was little congressional reaction."[720]

9.85 The Office of Technology Assessment (OTA), in 1986, produced a report on a survey of Federal agency use of electronic record systems. Regan summarises the findings of the survey as follows:[721]

> The OTA concluded that the widespread use of computerised databases, electronic record searches and matches, and computer networking was rapidly leading to the creation of a de facto national database containing personal information on most Americans.

In response, the Computer Matching and Privacy Protection Act was enacted by Congress in 1988.[722] The Act amended the Privacy Act 1974, and further amendments were made in 1990.

9.86 The information matching provisions in the New Zealand Privacy Act are modelled closely on the US Act. Under the US Act, Federal agencies involved in computer matching programmes (principally those relating to eligibility for Federal benefit programmes)[723] must negotiate written agreements with the other agencies that are participating in the programme, and those agreements must be approved by a data integrity board (which each agency conducting or participating in a matching programme must establish). Matching agreements must specify the legal authority and purpose of the programme, the justification for the programme and the anticipated results (including an estimate of any savings), and how matching under the programme is to be carried out.[724]

720 Priscilla M Regan *Legislating Privacy: Technology, Social Values, and Public Policy* (UNC Press, Chapel Hill, 1995) 87.

721 Priscilla M Regan *Legislating Privacy: Technology, Social Values, and Public Policy* (UNC Press, Chapel Hill, 1995) 95.

722 5 USC § 552a (o) – (u).

723 There are wide exemptions for law enforcement, intelligence, and tax purposes.

724 5 USC. § 552a (o).

9.87 A Government Accountability Office review of the implementation of the Act in 1993 identified deficiencies.[725] Apparently the cost-benefit analysis required before a programme is approved was often inadequate, and the data integrity boards did not provide adequate supervision.[726] A 2008 Government Accountability Office report on computer matching by the Inland Revenue Service is still not particularly encouraging.[727]

9.88 It should be noted that in addition to the Privacy Act and the Computer Matching and Privacy Protection Act, Congress has enacted the E-Government Act 2002.[728] Among other things, the Act requires Federal departments and agencies to conduct privacy impact assessments (PIAs) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form, or before initiating any new electronic data collections containing personal information on 10 or more individuals. A new computer matching initiative may therefore trigger the need for a PIA under this Act. However, OMB guidance on the Act indicates that a PIA is not required when all elements of a PIA are addressed in a matching agreement governed by the Computer Matching and Privacy Protection Act.[729]

Hong Kong

9.89 The Hong Kong Personal Data (Privacy) Ordinance, section 30, regulates data matching in Hong Kong. The Ordinance was enacted in 1995, but the data matching provisions did not come into force until August 1997. The Ordinance is overseen by the Privacy Commissioner for Personal Data. Unusually, the relevant provision of the Ordinance applies to data matching by the public and private sectors.[730] Data matching is defined as a comparison of two sets of personal data, each of which is collected for different purposes, where each comparison involves the personal data of 10 or more data subjects, the comparison is carried out using a computer programme designed and applied for performing the comparison process and not by manual means, and the end result of the comparison may be used, whether immediately or at any subsequent time, for the purpose of taking adverse action against any of the data subjects concerned. Data matching that does not fall within the definition could still be covered by the data protection principles and other provisions of the Ordinance.

725 Government Accountability Office *Computer Matching: Quality of Decisions and Supporting Analyses Little Affected by the 1988 Act* (GAO/PEMD-94-12, October 1993).

726 See further, Roger Clarke "Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism" (1995), available online at www.rogerclarke.com.

727 Government Accountability Office *Tax Administration: IRS Needs to Strengthen Its Approach for Evaluating the SRFMI Data-Sharing Pilot Program; a report to the Committee on Finance, U.S. Senate* (GAO-09-45, November 2008).

728 44 USC § 101.

729 Office of Management and Budget *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Memorandum M-03-22, Washington, D.C., 26 September, 2003).

730 The Law Reform Commission of Hong Kong report that preceded the Ordinance expressed particular concerns about "investigative data matching" that could lead to an adverse decision against an individual. This could arise in both the public and private sectors, for example in insurance and credit reporting. Law Reform Commission of Hong Kong *Report on Reform of the Law Relating to the Protection of Personal Data (Topic 27)* (Hong Kong, 1994) 121, 129–130.

9.90 A data user must not carry out a matching procedure unless all the individuals who are the subjects of the data to be matched have voluntarily given express consent to the matching procedure being carried out, or the Privacy Commissioner for Personal Data has consented to the matching procedure being carried out, or the matching procedure belongs to a class of permitted matching procedures gazetted by the Privacy Commissioner or is required or permitted by a specified law.[731]

9.91 The overwhelming majority of applications for the Privacy Commissioner's approval to a matching procedure appear to come from the public sector, and in relation to social security benefit, law enforcement, and tax matters. Very few applications for approvals or re-approvals appear to be refused, but conditions are often imposed.

RESTRICTIONS ON INFORMATION MATCHING STILL NEEDED

9.92 We noted earlier that one of the principal reasons why privacy legislation was enacted in the early 1990s was to authorise the exchange of information between certain government agencies for the purpose of combating fraud and abuse of the social welfare system, and subject those information exchanges to a system of controls, reporting and monitoring. As can be seen from our examination of subsequent developments, the scale and reach of information matching by government agencies has increased significantly since then.

9.93 The risks to individual privacy are consequently just as great, if not greater. As one commentator (albeit in the US context) has said: "the principle underlying the [Privacy Act 1974, (US)] – that individuals should be able to exercise control over information about themselves that they provide to the government – is a bedrock principle of individual privacy. That principle is at war with the practice of computer matching."[732]

9.94 The modern state could not function effectively without access to the vast amount of personal information provided directly by citizens or collected in other ways. Increasingly sophisticated technology provides the tools to use that information for socially beneficial purposes, such as improving service delivery, the more efficient use of resources, the protection of government revenue, and research. These and other benefits of information matching need to be balanced with the risks to privacy. Striking the right balance can build and maintain citizens' trust in government, providing the assurance that citizens can continue to provide the state with the information it needs to function, confident that their information will be protected and used appropriately.

731 Personal Data (Privacy) Ordinance (Cap 486) (HK), s 30(1).

732 John Shattuck "Computer Matching is a Serious Threat to Individual Rights" (1984) 27 Communications of the ACM 538.

9.95 The issue is neatly summarised by the Victorian Office of Privacy Commissioner as follows:[733]

> Addressing data matching is part of the larger challenge of ensuring that the collection and handling of personal information in a technological age is done according to longstanding values, including respect for privacy. In its Information Privacy Principles, Victoria has adopted well known international data protection standards. This is partly to build trust, partly to keep a check on potential abuse of power, and partly to ensure that the necessary data continues to be available. If people lack trust in authorities, or do not believe that abuses can be detected and checked, then they begin to act in self defence. They may provide false or incomplete data. This in turn reduces the quality of decisions based on the data. This is not in the public interest and, over time, it will corrode the legitimate tasks of public administration, for which personal information, aided by technology, is necessary.

9.96 We therefore have no doubt that controls on information matching by government agencies are still required and, subject to what we say below, we think the current controls appear to be working reasonably well. Based on the results of the Privacy Commissioner's audit regime and reports, compliance by agencies with the statutory requirements is high. On that basis, we can find no case for substantial change.

9.97 The New Zealand regime also compares favourably with the overseas regimes we have examined. The "openness, precision, and oversight" features rated so highly by the Victorian Office of Privacy Commissioner are of key importance. New proposals to enact information matching authorities are the subject of rigorous evaluation and debate. In comparison with more general principles or guidelines, the detailed statutory regime provides greater certainty to agencies as to what they can and cannot do. In that respect, Part 10 and Schedule 4 are effectively a statutory code of practice with respect to information matching.

9.98 We also consider that the Privacy Commissioner's oversight of information matching is appropriate, given the nature of information matching. Because of the remote connection between information matching programmes and the individuals whose data is matched, reliance on the normal individual complaint and enforcement mechanisms of the Privacy Act to curb or detect abuses is unlikely to be effective.

Q105 We consider that the current controls on information matching by public sector agencies are appropriate and should be retained. Do you agree?

733 Office of the Victorian Privacy Commissioner *Victorian Public Sector Data Matching Audit* (Melbourne, February 2005) 2.

OPTIONS AND PROPOSALS FOR CHANGE

Information matching and the private sector

9.99 The information matching provisions in the Privacy of Information Bill as introduced in 1991 applied to both the public and the private sector. The Bill as reported back by the Justice and Law Reform Select Committee limited the information matching provisions to the public sector, on the basis that information matching in the private sector could be regulated by code of practice if necessary.[734] This is reflected in section 46(4)(a), which provides that a code of practice may impose controls on information matching by agencies that are not public sector agencies.

9.100 In the absence of a code of practice, information matching in the private sector is therefore, for the most part, regulated by the privacy principles relating to the collection, use, and disclosure of personal information, and the use of unique identifiers.

9.101 The only code of practice that expressly addresses information matching in the private sector is the Credit Reporting Privacy Code 2004, rule 8(2) of which provides that:

> A credit reporter must, when undertaking a comparison of personal information with other personal information for the purpose of producing or verifying information about an identifiable individual, take such measures as are reasonably practicable to avoid the incorrect matching of the information.

9.102 By comparison with the detailed provisions of Part 10 and Schedule 4 of the Act, the code therefore leaves it very much to individual credit reporters to determine the reasonably practicable steps they must take to avoid incorrect matches. However, this must also be seen in the context of the restrictions on the kinds of personal information that credit reporters are lawfully able to collect, and therefore use for identity verification. Forms of unique identification such as a driver's licence cannot be used for this purpose.

9.103 Are there differences between public and private sector agencies in terms of how they collect, use, and disclose personal information, and the privacy risks arising therefrom, that justify different treatment in terms of restrictions on information matching? Public sector agencies will often have the power to compel people to provide personal information, whereas private sector agencies can usually collect information only by consent. However, in a number of situations an individual's ability not to provide information to an agency is not determined by whether the agency is public or and private. A person's choice is very limited when it comes to basic services provided by the private sector such as energy, telecommunications, and banking, and the terms of service tend to be the same for all providers. To obtain the service, the individual will usually have to provide the personal information requested by the provider, and agree to the terms and conditions that the provider specifies with respect to how that information may subsequently be used.

734 H Hancock (18 March 1993) 533 NZPD 14133.

9.104 Nevertheless, we are not in a position to say that there are sufficiently widespread and serious problems with the use of information matching by the private sector that restrictions similar to Part 10 and Schedule 4 should be extended to that sector. The Privacy Commissioner has not recommended it, nor has the Commissioner made or proposed any general or specific code of practice with respect to it (apart from the Credit Reporting Privacy Code). We need further information on this issue before coming to any firm conclusion, and welcome submissions on the point.

9.105 There are also options short of regulation that might be considered. One of these options is the issuing of guidelines by the Privacy Commissioner. Such guidelines would not be binding, but the Privacy Commissioner could take them into account in assessing compliance with the privacy principles.

9.106 Our proposal in chapter 6 to confer an audit power on the Privacy Commissioner is also relevant here. An appropriate audit power would enable the Privacy Commissioner to investigate current practices with respect to information matching in the private sector to see if any action is required.

Q106 We do not think that there is currently a case to impose detailed controls on information matching by private sector agencies. Do you agree? If not, can you provide examples of situations where a lack of controls has put people's privacy at risk?

A separate Data Matching Act

9.107 In *Necessary and Desirable* the Privacy Commissioner described Part 10 as "relatively technical."[735] We think this significantly understates its specialised, complex, and arcane nature. Further, unlike the rest of the Act (with the exception of Part 11 and Schedule 5, which deal with law enforcement information), Part 10 and Schedule 4 relate only to public sector agencies.

9.108 We consider that the technical, complex, and restricted nature of Part 10 means that it is out of place in a general information privacy statute. Most users of the Act will never need to refer to it, and it therefore clutters up the Act. On the other hand, Part 10 contains important privacy protections that justify statutory recognition. We therefore propose that Part 10 and Schedule 4 should not be included in a new Privacy Act but (as in Australia) enacted as a separate Act, along with the detailed changes we propose below. The new Act might be called the Privacy (Public Sector Data Matching) Act.

9.109 Even if Part 10 and Schedule 4 are enacted as a separate Act, it will be important to emphasise the new Act's privacy protection aspects and its continuing connection with the Privacy Act. This can be achieved through the inclusion of a purpose provision and appropriate cross-references between each Act.

735 *Necessary and Desirable* para 10.1.3.

Q107 We propose that Part 10 and Schedule 4 should be enacted as a separate Privacy (Public Sector Data Matching) Act. Do you agree?

Detailed changes

9.110 We think that a number of changes to Part 10 are necessary to clarify, modernise, and simplify its provisions. These go beyond just updating the structure, drafting style, and format, and introducing useful aids to clarity (such as a flowchart of the information matching process). A number of detailed recommendations have been made by the Privacy Commissioner in *Necessary and Desirable* and subsequent supplementary reports. Where appropriate, these recommendations are included here.

Widen scope

9.111 We noted above that Part 10 does not currently regulate all information matching by public sector agencies.[736] Except in certain limited circumstances, even where a specific statutory authority to undertake information matching exists, a public sector agency does not have to utilise that authority and comply with Part 10 if it can rely on an alternative source of authority (such as the privacy principles and their exceptions). There are "anti-avoidance" mechanisms in sections 108 and 109, but these are narrow.

9.112 Our present view is that Part 10 should apply to all information matching programmes undertaken by public sector agencies. An agency should not be permitted to undertake information matching (within the meaning of Part 10) unless there is a specific statutory authority for it to do so and it undertakes information matching under and in accordance with that authority and Part 10.

9.113 Such an extension would also put beyond doubt that information matching involving public registers is subject to the usual controls, even though personal information in a public register is publicly available information and therefore exempted from principle 2.[737] The extension should also rule out reliance by agencies on the general law enforcement information regime in Part 11 of the Act (or whatever regime replaces it) as authority to undertake information matching.

9.114 We note that this extension of Part 10 would formalise the existing understanding that public sector agencies will not conduct information matching without specific statutory authority, and that new proposals should be subject to a rigorous process of justification and assessment before any such authority is granted.

Q108 We consider that all information matching undertaken by public sector agencies should require specific statutory authority, and be covered by the controls in Part 10 and Schedule 4. Do you agree?

736 Paragraphs 9.32–9.35.

737 With respect to public registers, see New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008).

Definition of "adverse action"

9.115 The definition of "adverse action" in section 97 is of central importance to the operation of Part 10. Section 100 states that agencies can take "adverse action" against an individual on the basis of a discrepancy produced by an information matching programme in which the agency is involved. Sections 101 to 103 impose important procedural safeguards for individuals against whom agencies may take adverse action on the basis of a discrepancy.

9.116 The definition of adverse action states generally that it is any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual.[738] It then contains a non-exhaustive list of examples of decisions that fall within the term, such as a decision to cancel or suspend a social welfare benefit, to assess the amount of a tax or charge, or to investigate the possible commission of an offence.

9.117 While the list of examples is not exhaustive, the Privacy Commissioner, in *Necessary and Desirable*,[739] recommended that the definition be amended to include further examples of commonly occurring adverse actions. This would make the provision clearer and more helpful for agencies, and also as a consequence ensure that the procedural protections in Part 10 for individuals are complied with. It may well be thought that there are dangers in leaving it to an official to determine whether an action is adverse or not without clear guidance. The two kinds of decision identified by the Privacy Commissioner are a decision to impose a penalty, and a decision to recover a penalty or fine imposed earlier.

9.118 The examples listed in the definition of "adverse action" tend to reflect the kinds of action that were the focus of the first tranche of information matching authorities. As indicated above, the number and scope of these authorities have increased significantly since then. Except for the addition, in 2004, of a reference to certain decisions relating to immigration matters (such as a decision to deport), the list of examples has not otherwise been amended. We tend to support the Privacy Commissioner's recommendations for additions to the list. However, we also consider that paragraphs (a) to (d) of the list, which relate to decisions with respect to monetary payments, could be condensed. Otherwise there is a danger that the list of decisions could become too long and unwieldy, and therefore less helpful.

9.119 We are also aware of a suggestion that the definition of "adverse action" should be amended to make it clear that information matching programmes that have a beneficial consequence for individuals (such as entitlement to a benefit not being claimed), or no adverse consequence (that is, a neutral consequence), are expressly excluded. This, it is said, would remove confusion among agencies as to whether or not they must comply with provisions such as the notice requirement in section 103, and when information provided for or derived from an information matching programme must be destroyed.

738 Privacy Act 1993, s 97.

739 *Necessary and Desirable* recommendation 117.

9.120 An example might be an information matching programme authorised by section 78A of the Births, Deaths, Marriages, and Relationships Registration Act 1995. Under this provision, the Registrar-General can obtain address information from the Ministry of Social Development in order to assist in locating and contacting the mothers of children whose births are unregistered so that their births may be registered. It is hard to see how registering an unregistered birth could be considered as an action that "may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual".

9.121 It seems obvious that an action that has a beneficial or neutral consequence for someone is not an "adverse action". We are not convinced that the suggestion to expressly exclude such actions from the definition has merit, and are more inclined to think that the clarification and simplification of sections 101 to 103 and Schedule 4 will serve the same purpose. Nevertheless, we would welcome any comments on the matter.

Q109 We propose that the list of examples of what constitutes "adverse action" against an individual should be extended to include a decision to impose a penalty, and a decision to recover a penalty or fine imposed earlier. Do you agree? Should any other changes be made to the list of examples?

Q110 We are currently of the view that the definition of adverse action should not be amended to clarify that information matching programmes that have a beneficial consequence for individuals or no adverse consequence are expressly excluded. Do you agree?

Computerised and manual matching

9.122 In comparison with other jurisdictions, the New Zealand information matching provisions are unusual in applying to both computerised and manual matching. The US and Hong Kong legislation specifically apply only to computerised matching. The Australian Data-Matching Program (Assistance and Tax) Act 1990 does not expressly exclude manual matching, but the provisions relating to data matching and matching cycles clearly contemplate computer matching.

9.123 The Privacy Commissioner originally recommended in *Necessary and Desirable* that manual matching be excluded from Part 10 on the basis that the risks to privacy from data matching arise primarily from the automated or computerised nature of the exercise, and that no manual matching programmes had been brought within the ambit of the Part. This recommendation was subsequently withdrawn by the current Privacy Commissioner, because some computerised matching programmes may have a manual element. Removing manual matching entirely from Part 10 might therefore reduce the safeguards imposed by the Part.

9.124 We are inclined to the view that focusing Part 10 on computerised matching is appropriate and desirable, since that is where the primary risk to privacy lies. We therefore tend to the view that information matching programmes that consist of the manual comparison of personal information should be excluded from coverage. To the extent that some computerised matching programmes may have a manual element, it should be made clear that these are still covered. Again, we would welcome comments on this issue.

Q111 We propose that the controls on information matching programmes by public sector agencies should be focused on computerised/automated matching, and manual matching should no longer be covered (computerised information matching with a manual component would continue to be covered). Do you agree?

Information matching guidelines

9.125 Under section 13(1)(f) of the Act, the Privacy Commissioner has the function of scrutinising legislative proposals involving the collection or disclosure of personal information by public sector agencies for the purposes of an information matching programme. In undertaking this scrutiny, the Privacy Commissioner is to have particular regard to the "information matching guidelines" set out in section 98.

9.126 The Privacy Commissioner has made three recommendations for amendment to section 98, designed to sharpen the analysis undertaken by agencies in preparing a proposal and so provide the Commissioner with better information on which to scrutinise the proposal.[740] The recommendations are as follows:

- Section 98(c) requires an assessment of whether or not an alternative means of achieving the objective of the proposed information matching programme would result in significant and quantifiable monetary savings, or in other comparable benefits to society. However, the provision does not require a consideration of whether or not the alternative means of achieving the objective would be more or less privacy-intrusive than the proposed programme. This is clearly an important consideration in deciding whether or not the alternative is preferable, and should be added.
- Section 98(e) requires an assessment of whether or not the proposed programme involves information matching on an excessive scale. In making this assessment, regard is to be had to the number of agencies to be involved in the programme and the amount of detail about an individual that will be matched. Additional considerations that should be added to section 98(e) are the amount of information disclosed as a result of a successful match, and the frequency of matches to be carried out under the programme.
- Agencies should be required to examine their proposed information matching programme against the requirements of Part 10, as well as the requirements of the privacy principles and the information matching rules.

740 *Necessary and Desirable* 312–316, recommendations 122–124.

9.127 We agree with these recommendations.

9.128 It goes without saying that the ability of the Privacy Commissioner to properly assess a proposed information matching programme in accordance with section 98 depends in large part on the information provided to the Commissioner by the relevant agencies sponsoring the proposal. It has been suggested to us that a statutory requirement on the sponsoring agencies to supply the Commissioner with a written assessment of their proposal in the form of a "programme protocol" would highlight the need for agencies to undertake the necessary policy spadework when developing a proposal, and facilitate assessment of the proposal by the Commissioner.

9.129 As we understand it, the programme protocol would be a comprehensive document containing all relevant information about the proposed information matching programme. It would address each of the matters set out in section 98, as well as how the other control and reporting requirements in Part 10 and Schedule 4 would be complied with.

9.130 The programme protocol process is seen as a way of streamlining and bringing together a number of disparate processes so as to make the approval process for information matching programmes not only more efficient, but also more transparent. It is envisaged that the protocol would be made publicly available at the end of the process, and so facilitate compliance with the requirements of information matching rule 1 to promote public awareness of the programme.

9.131 We support the suggestion for a mandatory programme protocol procedure but we are open to alternative views on this point.

> Q112 We propose that the information matching guidelines in section 98 should be amended to require a mandatory protocol procedure so that the Privacy Commissioner has better information on which to assess proposals for new information matching authorities. Do you agree?

Section 103: Notice of adverse action

9.132 Section 103(1) currently provides that an agency must not take adverse action against an individual on the basis of a discrepancy produced by an information matching programme unless it has first provided notification, telling the individual that he or she has five working days from receipt of the notice to show why the action should not be taken, and waited for those five working days to expire. This is an important part of the post-match verification process, as it gives time for the individual to respond and point out if there has been an error.

9.133 The Privacy Commissioner recommended that the notice period be increased to 10 working days, on the basis that five working days is too short and a longer period would enhance the protection of individual rights that section 103 confers.[741] The equivalent period in Australian legislation is 28 days (20 working days).[742]

741 *Necessary and Desirable* recommendation 128.

742 Data-matching Program (Assistance and Tax) Act 1990 (Cth), s 11. In some circumstances, however, the Australian Act permits action to be taken without giving notice.

9.134 We also note that section 103 currently exempts certain information matching programmes from the requirement to wait until the expiry of the specified period before taking adverse action.[743] The requirement in section 103 has also been expressly overridden by other legislation.[744] It has been suggested that an alternative to specific statutory exemptions would be to confer a discretion on the Privacy Commissioner to shorten or waive the notice period in appropriate cases. We think that this would provide greater flexibility than the current method of blanket statutory exemptions and specific statutory overrides, and permit tailor-made arrangements that appropriately balance administrative considerations and the need to safeguard the interests of individuals.

9.135 We tentatively support both suggestions. We consider a 10-day notice period more appropriate. The provision of a discretion for the Privacy Commissioner to shorten or waive the notice period in section 103 should replace the need for statutory exemptions and overrides.

Q113 We propose that the period of notice that should be given by an agency before it takes adverse action against an individual on the basis of the results of an information matching programme should be increased from five working days to 10 working days. The Privacy Commissioner should also be empowered to shorten or waive the notice period in appropriate cases. Do you agree?

Privacy Commissioner oversight, reporting, and review

9.136 As set out above, the Privacy Commissioner plays a key role in overseeing the operation of information matching programmes, reporting to Parliament on their compliance with Part 10, and reviewing information matching authorities. For the most part, these processes work well. We have the following suggestions for enhancing them.

9.137 Currently, the Privacy Commissioner's annual report must include a detailed report on each information matching programme carried out during the relevant year. The Commissioner has recommended delinking the general annual report from the annual information matching reports, since finalisation of the Commissioner's annual report is unnecessarily delayed while waiting for the information matching reports to be received from agencies and analysed by the Commissioner. The Commissioner's report on the information matching programmes would be presented separately to Parliament.[745] We agree with this recommendation.

743 See *Necessary and Desirable* recommendation 129. The Privacy Commissioner considered that the exemption in section 103(1A) was unnecessary and objectionable, and should be repealed.

744 For example section 180C of the Corrections Act 2004 permits immediate suspension of benefits, allowances, and student loans as a result of a discrepancy produced by an information matching programme involving prisoners.

745 *Necessary and Desirable* recommendation 131.

9.138 We have also considered the section 106 requirement on the Privacy Commissioner to review each information matching authority every five years. Two reviews covering six information matching programmes have been completed since 1994. Resourcing constraints have prevented both the current and the previous Privacy Commissioner from undertaking the regular reviews of information matching authorities required by section 106.

9.139 The review of authorising provisions for information matching is an important part of the overall system of oversight of information matching. Since these authorising provisions constitute an exception to the privacy principles, it is appropriate that each authority is regularly reviewed to establish whether or not it is still needed, whether or not the expected benefits from the programme are being realised and are sufficient to justify the inroads into privacy that the programme involves, and whether or not the actual operation of the programme over the review period provides sufficient confidence that the risks to privacy arising from the programme have been sufficiently well-managed to justify the continued existence of the programme.

9.140 In the absence of additional resourcing, an alternative to the review process might be considered. One option would be to "sunset" all information matching authorisations after a specified period (perhaps five years). The authority would lapse unless renewed by Parliament. The relevant agencies would have to justify the continuation of the authority to Parliament. A variation on this approach would be to provide for the life of information matching authorities to be extended by Order in Council, but provide that extensions could only be granted if the Privacy Commissioner had reviewed an Information Matching Privacy Impact Assessment and programme protocol for the programme and recommended that the extension be granted.

9.141 In addition, where the Privacy Commissioner does undertake a section 106 review, there is no requirement for the Government to respond to the Privacy Commissioner's report. We suggest that there be a requirement on the Government to present a response to the House within six months of the presentation of the Commissioner's report.

Q114 We propose that the Privacy Commissioner should be able to present a separate report to Parliament each year on his or her monitoring of information matching programmes, rather than include this in the Commissioner's annual report. Do you agree?

Q115 We propose that, in the absence of increased resources to enable the Privacy Commissioner to undertake the required 5-yearly reviews of information matching authorities under section 106, each authority should be sunsetted so that it expires after five years unless (a) renewed by Parliament, or (b) extended by Order in Council made on the recommendation of the Privacy Commissioner. Do you agree? If so, which option do you prefer?

Q116 We propose that, if the Privacy Commissioner continues to undertake reviews of information matching authorities, there should be a requirement on the Government to respond to the Commissioner's report within six months of the presentation of the report. Do you agree?

Exemptions for the Inland Revenue Department

9.142 Section 101 and information matching rule 6 require agencies to either use information produced by an information matching programme to take adverse action against an individual, or destroy the information. The information cannot simply be held by the agency indefinitely. Adverse action must be commenced within 12 months from the date the information was produced, and the information must be destroyed when it is no longer needed for the purposes of taking adverse action against any individual. The source information disclosed for the purpose of the programme must also be destroyed if it does not reveal a discrepancy, or once it is no longer needed for the purposes of taking any adverse action.

9.143 The Inland Revenue Department (IRD) is currently exempt from all of these requirements with respect to every information matching programme. In *Necessary and Desirable*, the then Privacy Commissioner queried this blanket exemption.[746] He considered that any exemption for the IRD, if justified, should be conferred in the context of individual information matching authorities, and restricted to circumstances where the IRD is the end user of the information produced by a programme.

9.144 We think that a wider reconsideration of the current blanket exemption for the IRD is justified. It is hard to see why every agency other than the IRD is required to commence adverse action against an individual within 12 months from the date information is derived from an information matching programme. We share the Privacy Commissioner's concerns about the ability of the IRD to retain any information used in or derived from an information matching programme in which it is involved, regardless of whether it is the recipient or provider of the information.

9.145 It is our current view that the IRD's blanket exemptions should be repealed. Specific exemptions related to individual information matching authorities should be provided instead, if a good case can be made for them. Again, we welcome any comment on this point.

Q117 We propose that the Inland Revenue Department should no longer have a blanket exemption from the requirements to commence adverse action against an individual within 12 months, and to destroy personal information provided for or derived from an information matching programme once it is no longer needed. Specific exemptions for individual information matching authorities should be provided instead, if these can be justified. Do you agree?

746 *Necessary and Desirable* para 10.6.4.

Information matching rules

9.146 The information matching rules in Schedule 4 are a mixture of general and detailed, technical requirements. They can be amended or replaced by Order in Council made in accordance with the recommendations of the Privacy Commissioner under section 107. However, some of the rules are so important or fundamental to the fair operation of information matching programmes that we think they ought to be stated in the body of the Act itself. This would mean that only Parliament could change them. We put the following rules in this category:

- *Rule 1*: This rule requires agencies involved in authorised information matching programmes to take all reasonable steps to ensure that individuals who will be affected by the programme are notified of it. Openness and transparency with respect to information matching programmes are important accountability mechanisms.
- *Rule 7*: This rule prohibits agencies involved in an information matching programme from linking or merging the information used in the programme to create a new separate permanent register or databank of information about the individuals whose information has been subject to the programme. The rule is designed to prevent government agencies from using information matching to build up comprehensive profiles on individual citizens.

9.147 Those rules that are not of such a fundamental nature should remain in a schedule of the Act, and be subject to amendment or replacement by Order in Council. The technical nature of the rules justifies this degree of flexibility. Greater flexibility could also be introduced by authorising the Privacy Commissioner, in particular cases, to waive certain requirements in the rules, or grant exemptions from the requirements subject to conditions. This would reflect the fact that the rules must cover a wide variety of information matching programmes, and permit the Commissioner to tailor the information matching rules to cater for individual programmes.

9.148 We do not make further detailed recommendations about the information matching rules here. The Privacy Commissioner issued special reports in 2001 and 2003 recommending replacement of the information matching rules. These recommendations followed on from and built on the Commissioner's recommendations in *Necessary and Desirable*. The Commissioner described the objectives of the revision of the rules as follows: to express the existing rules more clearly; to provide new flexibility to recognise the diversity in authorised information matching programmes; to better integrate Part 10 and the rules; to use new concepts where appropriate to simplify meanings; and to enhance protections of individuals.

9.149 We would expect these recommendations to be taken into account in the preparation of any new legislation about information matching.

Q118 We propose that the current information matching rules requiring publicity and notice of information matching programmes, and prohibiting the creation of separate databanks, should be stated in the body of the Act itself. Do you agree? Are any other information matching rules so important that they should also be included in the Act rather than a schedule?

Future-proofing Part 10

9.150 Problems are sometimes encountered with respect to the application of Part 10 where agencies merge or their functions change.

9.151 One way of addressing this issue might be to empower the making of regulations amending the list of specified agencies in section 97 to ensure that the information matching controls in Part 10 continue to apply when agencies are reorganised.

Q119 Should the Act provide for the making of regulations amending the list of specified agencies in section 97 to ensure that the information matching controls in Part 10 continue to apply when agencies are reorganised?

Other issues

Q120 Do you have any other comments or suggestions about information matching?

Chapter 10
Information sharing

10.1 In the last chapter, we examined information matching by public sector agencies. As we have seen, this is a specialised form of information sharing and has its own regime in the Privacy Act. This chapter examines the broader issue of the sharing of information between public sector agencies. The sharing of personal information for a variety of purposes is vital to the functioning of our society, as a report in the UK has recognised:[747]

> the use and sharing of personal information are now permanent features of modern life, supported by mushrooming technological advances in the storage, analysis and use of large data sets. Public, private and voluntary sector organizations will continue to require access to personal information in order to provide goods and services, combat crime, maintain national security and to protect the public.

However, such sharing has major implications for privacy. A former Information and Privacy Commissioner of the Canadian province of Ontario has explained that:[748]

> Sharing personal information between two organizations runs counter to two of the most fundamental principles of data protection – that personal information should be collected directly from the individual to whom it pertains, and should only be used for the purpose for which it was collected [with limited exceptions]. … Therefore, where possible, sharing should not occur without exploring less privacy-invasive means of meeting a specific objective.

The challenge, then, is to facilitate the sharing of personal information for individually or socially beneficial purposes while ensuring that privacy is appropriately protected.

10.2 This chapter looks at how information sharing works within the current legal framework; problems identified by government agencies and researchers; and approaches to information sharing overseas. We then set out some guiding principles for reform, and put forward a range of options for reform.

747 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) 9–10.

748 Tom Wright, former Ontario Information and Privacy Commissioner *Model Data Sharing Agreement* (1995) 1.

BACKGROUND

10.3 "Information (or data) sharing" is not a term of art, although it is in fairly common usage both in New Zealand and elsewhere. It is mainly about the disclosure of information by one agency to another, often by way of mutual exchange. But in some instances it goes further. For example, it can include the case where several organisations use the same database: the old Wanganui Computer was a complex example of this.[749] In this chapter we use the term in its widest sense, although most often the references will simply be to the disclosure of information by one agency to another.

10.4 Information sharing can in some instances be a precursor to information matching, and may sometimes also be carried out to facilitate data mining, which we introduced in the last chapter. Unless permitted under Part 10 (information matching), Part 11 (which relates to law enforcement information), a code of practice, an authorisation granted under section 54, or a provision in some other legislation, information sharing is generally covered by the ordinary privacy principles. One of the key issues raised in this chapter is whether the privacy principles are sufficiently clear or flexible to enable the sharing of information between government agencies when this is necessary or desirable in the public interest or the interests of an individual.

10.5 We focus on information sharing between public sector agencies because it is in the public sector where the issues about the adequacy of the privacy principles have been raised. That is not to say that we are not interested in hearing about problems with the application of the privacy principles to the private sector in this area. If private sector agencies and non-governmental organisations (NGOs) also have problems in this area, we certainly want to hear about them.

10.6 As with information matching, this is an area where technological advances are hugely significant. The difficulties of locating and sharing personal information between public sector agencies when the information is stored in individual paper files held in each agency are swept away when the information is held in digital form and is accessible remotely from anywhere, without the need to physically transfer the information from agency to agency. The authors of the *Data Sharing Review Report* in the UK had this to say:[750]

> Technological advances have had a dramatic impact on data collection and management. Ever larger databases, powerful search and analysis facilities, and the increased (and almost infinite) storage capacity of modern IT systems belong to a very different world from filing cabinets stuffed with paper. It is simple to share, search and interrogate huge datasets electronically, although not so simple to do this safely and securely.

749 The Wanganui computer system was established by the Wanganui Computer Centre Act 1976 (now repealed). It held information relating to law enforcement that was available to most justice sector agencies, including Police, Justice and Land Transport.

750 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) 44.

10.7 It is also an area where the configuration of the public sector at any particular time may have an impact. How the public service is structured in terms of the particular agencies that exist and the functions assigned to them is often a matter that is dependent on the policies of the particular government in power at the time. The configuration of the public sector at any particular time and the particular functions that an agency has are relevant to the purpose for which an agency collects personal information. Because the purpose for which information is collected can be a key determinant of whether the information can be used or disclosed by the agency to other agencies, a change in the configuration of the public sector may impose barriers to the desirable use or sharing of personal information by the reconfigured agencies.[751]

10.8 There are significant tensions between competing interests here. It is often frustrating for citizens to have to provide the same personal information to different agencies for similar or related purposes. The frustration may be exacerbated by an assumption (whether reasonable or not) that having provided information to one agency, the information is available to other agencies because they are all part of government, and so much information is held in digital form that "it must be available to other agencies". The growing availability of online government services, and a more "citizen-centred" approach to the delivery of government services are responses to this issue.[752]

10.9 At a general level, the Privacy Act recognises these tensions. Section 14 directs the Commissioner, in exercising his or her functions, to recognise the right of Government to achieve its objectives in an efficient way. Section 7 addresses the relationship of the Privacy Act to other legislation.

10.10 On the other hand, there are the basic principles in the Privacy Act relating to the purpose of the collection and disclosure of personal information and consent to disclosure. The Act justifiably establishes a reasonably high threshold for overriding these principles. As with information matching, information sharing carries significant risks for the citizen. One risk is:[753]

> the ease with which inaccurate or incomplete information can, through data sharing programs, be replicated and widely distributed across various databases. Privacy laws give citizens the right to access their personal information and ask for it to be corrected, but in complex data sharing arrangements and complex systems, how will citizens even know where their information is or what's been done with it? This is a vexing question for which solutions must be found.

751 This is less likely to be an issue for agencies in the law enforcement sphere, because of the specific mechanisms in the Privacy Act relating to the use and disclosure of personal information for law enforcement purposes.

752 An example of the integrated service delivery model is the "igovt" initiative. This is a set of all-of-government services enabling people to interact securely with government agencies online. The first part of this service, "igovt logon service", which provides a single logon to access government services without a person's identity being shared, has already been launched. A further part of the service, the "igovt identity verification service", will enable people to verify their identity to government agencies online and in real time to a high level of confidence. See further www.i.govt.nz.

753 David Loukidelis, former Information and Privacy Commissioner for British Columbia "Where Angels Fear to Tread – Privacy in the Brave New World of Data Sharing" (Speech delivered at Life in a Digital Fishbowl – A Struggle for Survival or a Sea of Opportunity?, 10th Annual Privacy and Security Conference, Victoria, British Columbia, 4 February 2009).

> Another risk is …our tendency to often attribute excessive reliability, sometimes almost infallibility, to the products of technology, to confuse information for knowledge, information for proof. And when the product of the technology is a new picture of an individual, based on isolated bits of personal information that may or may not be an accurate reflection of that individual, citizens should be worried.

10.11 There is a paradox in all this. On the one hand, the failure of government agencies to share information can result in significant public reaction, and even outrage, particularly in circumstances where there are tragic outcomes (such as the death of a child from abuse). On the other hand, the same reaction can result when government agencies share information in circumstances that the public regards as inappropriate. Achieving the correct balance is not easy.

10.12 As can be seen from our discussion of overseas approaches below, New Zealand is not alone in grappling with this issue. A number of countries have confronted the issue in the context of initiatives to prevent or detect terrorism, where privacy interests generally tend to give way in the face of threats to the security of the state and the safety of its citizens. In other contexts, such as law enforcement, social welfare, and taxation, the interests are more finely balanced. Particularly problematic are government initiatives that have a proactive "paternalistic/beneficial" motivation behind them, such as multi-agency targeting of assistance to so-called "dysfunctional" families or sections of the community, where the individuals might not want to be "helped". (Sometimes, however, vulnerable persons simply do not know of the support available: they might indeed want to be helped if the possibility could be brought to their attention.)

10.13 The issue of information sharing has often surfaced overseas in the context of, or at the same time as, large-scale mishandling or loss of sensitive personal information by public and private sector agencies.[754] (We examine particular responses to privacy issues arising from data loss in chapter 16, which relates to data breach notification.) Questions as to the appropriate sharing of personal information have therefore been coupled with serious concerns about the ability of agencies to safeguard personal information from unauthorised disclosure or loss.

10.14 Both issues highlight the importance of public trust in government. If citizens are suspicious about what information about them is shared, then they may cease cooperating and providing information.

10.15 This then raises the issue of transparency or openness around the sharing of personal information by government agencies. In the context of information matching, the Privacy Act provides that agencies involved in an information matching programme must take all reasonable steps to ensure that individuals who will be affected by the programme are notified of it, unless that would be likely to frustrate the objective of the programme. With the exception of the general provisions of principle 3, there is no equivalent obligation on agencies in relation to information sharing. Greater openness and reporting might help to allay citizens' suspicions about what government agencies are doing with their personal information, and maintain or enhance trust and confidence in government.

754 See, for example, United Kingdom Cabinet Office *Data Handling Procedures in Government: Final Report* (London, June 2008).

10.16 The Australian Law Reform Commission (ALRC) had this to say about information sharing in its review of Australian privacy law:[755]

> It is undesirable that inconsistent and fragmented privacy laws prevent appropriate information sharing. Information-sharing opportunities, which are in the public interest and recognise privacy as a right to be protected, should be encouraged. Rather than preventing appropriate information sharing, privacy laws and regulators should encourage agencies and organisations to design information-sharing schemes that are compliant with privacy requirements.

10.17 We agree, and seek in this chapter to identify ways in which the New Zealand Privacy Act might better facilitate appropriate public sector information sharing within a framework of openness, transparency, and accountability while at the same time according appropriate weight to privacy values.

CURRENT FRAMEWORK

Introduction

10.18 To illustrate the nature of the issues raised in this chapter, we begin by setting out a number of examples where questions about the ability of agencies to share information might arise. We then examine how the Privacy Act might apply in each situation.

Example 1

10.19 A convicted offender is about to be released from prison, subject to conditions as to where the offender is to live. Can the Department of Corrections alert the Police in the area in which the offender will live so that they can keep an eye on him to make sure he does not reoffend?

10.20 Schedule 5 of the Privacy Act permits the Police to have access to Department of Corrections' records of prisoners, but only to information about the location and date of release of the prisoner. With respect to community based sentences, sentences of home detention, and conditions of release, Police access is limited to the person's area of reporting, and in the case of a person released from a prison, the conditions of the person's release.

10.21 If the Department of Corrections has serious concerns that the offender will reoffend on release, then principle 11(e)(i) might permit disclosure of the information on the grounds that it is necessary to avoid prejudice to the maintenance of the law by preventing the commission of an offence. Disclosure might also be permitted under principle 11(f) if the person is considered to pose a serious and imminent threat to public safety or to the life of any individual.

10.22 Sections 181A and 182A of the Corrections Act 2004 authorise certain agencies, including the Department of Corrections and the Police, to enter into information sharing agreements with respect to "highest risk offenders" and "child sex offenders". Information can be disclosed under these agreements before the offender's release from prison. The purposes for which the information may be released are set out in the Act.

755 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 13.11.

10.23 For highest-risk offenders, the purposes for which personal information can be disclosed under an information sharing agreement are:[756] to assist the monitoring of compliance with their conditions of release; to assist in facilitating their rehabilitation; to facilitate their reintegration into the community; to manage the risk that they may commit further offences; to identify any increased risk that offenders may breach their conditions or will commit further offences.

10.24 For child sex offenders, the purposes for which personal information can be disclosed under an information sharing agreement are:[757] to monitor compliance by the child sex offender with his or her release conditions or other conditions; to manage the risk that the offender may commit further sexual offences against children; to identify any increased risk that the offender may breach his or her conditions or will commit further sexual offences against children; to facilitate the reintegration of the offender into the community.

10.25 The purposes for which personal information can be disclosed about highest-risk offenders and child sex offenders are therefore wider in certain respects than the purposes permitted by the exceptions to principle 11, although in some instances they overlap.

Example 2

10.26 A person has incurred debts to a number of different government agencies. He owes outstanding fines to the Ministry of Justice, arrears of income tax to the Inland Revenue Department, arrears of rent to Housing New Zealand Corporation, and an overpayment of a social welfare benefit to the Ministry of Social Development. The agencies want to work together in planning how the person can repay his debts to each agency, and in assisting the individual to avoid getting into debt in the future. Information that would need to be shared with each agency would be the identity of the debtor, the amount of the debt and repayment arrangements, the individual's overall financial position, and the circumstances that gave rise to the debt.

10.27 It is unlikely that the purpose of the collection of personal information about the individual by each agency would include the use or disclosure for the collaborative purpose envisaged here. Under the Privacy Act, it would therefore not be possible for each agency to share this information with the other agencies, without the person's consent. Agencies would not be permitted to disclose to each other the names of individual debtors, to enable them to identify who their common clients were, so that they could approach these clients and seek their consent to participation in the programme.

10.28 An information matching programme could be used to identify common clients of each agency, but this would require a legislative authority.

10.29 The Ministry of Social Development, in its 2008 Briefing to the Incoming Minister,[758] noted that there were a number of things social services agencies could do better if they could share client information more easily. These included preventing the creation or exacerbation of debt.

---

756 Corrections Act 2004, s 181A(3).

757 Corrections Act 2004, s 182A(3).

758 Ministry of Social Development *Briefing to the Incoming Minister: Organisation briefing* (Wellington, 2008) 36.

Example 3

10.30 A group of agencies identify the need to improve coordination between youth justice agencies and better coordinate service delivery to young offenders so as to prevent offending and reduce reoffending. The core agencies involved are Child Youth and Family (CYF), Police, Education and Health. Other government agencies and some NGO agency representatives might also need to participate.

10.31 Meetings of the agencies would involve: general discussions about service co-ordination, policies and issues, without reference to individual cases; discussions about service co-ordination, policies and issues where an individual's case information is used to illustrate a particular problem (often undertaken as retrospective reviews of cases); and case management discussions to resolve an operational problem relating to a particular individual or individuals.

10.32 Such an initiative is already operating in the form of Youth Offending Teams (YOTs).[759]. Ministry of Justice advice on the application of the Privacy Act to the operation of YOTs is as follows:[760]

> There would appear to be adequate existing legal mechanisms to enable YOTs to function effectively and to discharge their intended functions, namely that of a strategic overview of youth justice in a YOT's local area. These primarily rely on the exceptions to IPP/HIPR 11.

Discussion

10.33 The following analysis assumes that the ability of agencies to share information is to be determined solely by reference to the privacy principles. This assumes that authority to share is not conferred by a code of practice issued under Part 6,[761] an authority granted by the Privacy Commissioner under section 54,[762] an information matching authority under Part 10,[763] the law enforcement provisions in Part 11 and Schedule 5,[764] or a provision of some other legislation.[765]

10.34 The passing of personal information from one agency to another agency involves the disclosure of information by one agency and the collection of information by the other, as well as the use of information by both agencies. Information sharing therefore engages principles 1, 2, 3, 4, 10 and 11.

10.35 With respect to the collection of personal information, consideration needs to be given to the following:

- In terms of principle 1, is the information collected for a lawful purpose connected with a function or activity of the agency, and is the collection necessary for that purpose?

759 For more on YOTs see www.justice.govt.nz/policy-and-consultation/youth/youth-offending-strategy.

760 Ministry of Justice *Youth Offending Teams e-flash 12* (March 2008) 4.

761 See further the discussion in chapter 7.

762 See further the discussion in chapter 5.

763 See further the discussion in chapter 9.

764 See further the discussion in chapter 12.

765 See paragraphs 10.39–10.40 below.

- In terms of principles 2 and 3, why is this not a case where the information should be collected directly from the individual concerned, and where that individual is made aware of the fact of collection, the purpose of collection, and the other information required by principle 3?
- In terms of principle 4, is the collection of information by this means unlawful, unfair, or intrusive to an unreasonable extent upon the personal affairs of the individual concerned?

10.36 With respect to the use or disclosure of personal information, principles 10 and 11 require consideration of the following:

- In terms of principle 10, is the use of the information consistent with the purpose in connection with which it was obtained? If not, does one of the exceptions in principle 10 allow use for another purpose?
- In terms of principle 11, is the disclosure of the information to a person, body, or agency permitted by one of the grounds set out in that principle?

10.37 In some cases, the answer on both sides of the equation may be straightforward in that the individual concerned has authorised the sharing, both in terms of collection and use or disclosure; or the disclosure or use of the information may match the purposes in connection with which it was collected, or be directly related to one of those purposes. In the absence of consent or a matching purpose, potentially rather more complex questions arise in terms of whether or not their absence can be overridden by other interests. The ones most likely to be in issue are the need to avoid prejudice to the maintenance of the law, the enforcement of a law imposing a pecuniary penalty, the protection of the public revenue, the conduct of proceedings before a court or tribunal, or the need to prevent or lessen a serious and imminent threat to public health, public safety, or the life or health of the individual concerned or someone else.

10.38 There is no doubt that the complexity of some situations will pose a significant challenge for agencies in their decision-making processes.[766] There are other consequences. A lack of confidence that it is able to make the correct decision, and sustain it in the face of subsequent scrutiny by the Privacy Commissioner, might lead an agency to adopt "defensive decision-making". The "safe option" is not to share the information, but at the risk of jeopardising other interests. Alternatively, the agency might decide that the other interests should prevail, regardless of what it considers the Act requires. In both cases the Act is potentially brought into disrepute as failing to strike the right balance between privacy and other competing interests.[767] Tensions will probably continue to exist even if the Privacy Act is amended.

766 A good example is whether or not medical staff treating a suicidal patient in the community should inform the patient's family/whānau, especially where the patient expressly asks them not to. See the decision of the Health and Disability Commissioner in Case 08HDC08140, available on the Commissioner's website www.hdc.org.nz. In that case, the Commissioner held that, despite the fact that the patient was "absolutely adamant" that his family not be involved, "sometimes an individual's safety should override his or her privacy, and family or caregivers should be involved to help provide a safe environment for recovery". There have been several recent cases where New Zealand coroners have expressed concern in similar circumstances.

767 See, for example "Privacy broken to save lives: Police bend rules in battle to curb domestic violence" (19 August 2008) *Dominion Post* Wellington.

Specific legislative authorities for information sharing

10.39 In a number of cases, Parliament has legislated to empower or facilitate information sharing. We have already mentioned sections 181A and 182A of the Corrections Act 2004, which provide for information sharing about highest-risk offenders and child sex offenders. Another example is section 283 of the Injury Prevention, Rehabilitation, and Compensation Act 2001, which provides that the Accident Compensation Corporation may provide information about claimants and other persons to the Department of Child, Youth and Family Services if the Corporation believes on reasonable grounds that it is reasonably necessary for the purpose of preventing or limiting injury to children or young persons arising through unlawful activity. Information must be provided in accordance with an agreement between the Corporation and the chief executive of that department.[768]

10.40 There are advantages and disadvantages in enacting specific legislative authority to share information. On the one hand, it means that agencies are relieved from the task of applying the general provisions of the Privacy Act to a specific case. On the other hand, the existence of a specific authority in one context may cast doubt on the lawfulness of data sharing in situations not covered by the authority. Confusion, rather than certainty, may be the ultimate outcome.[769]

Previous work within government on an information sharing mechanism

10.41 A significant input into this chapter has been work done between 2005 and early 2008 by the Ministry of Justice and other government agencies on the development of a new government information sharing mechanism. The catalyst for this work was a view among some agencies that the Act impeded desirable co-operation among agencies by unnecessarily preventing information sharing, or imposing high compliance costs on agencies in implementing information sharing arrangements. A further criticism of the Act was that it failed to provide clear guidance to agencies on when they could or could not share information.

10.42 It was subsequently agreed that the issue of information sharing between Government agencies should be included in the Law Commission's review.

10.43 The Privacy Commissioner has investigated the option of developing a code of practice under the existing Privacy Act provisions, but has tentatively concluded that such a code is not appropriate at this point. However, she has not ruled out the possibility in future, depending on the reform directions taken as a result of this Law Commission review.

768 A further example is section 36 of the Passports Act 1992.

769 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) para 5.29.

What problems have been identified by public sector agencies?

10.44 This section sets out the issues or problems that have been raised with respect to data sharing between public sector agencies.

Privacy Act does not fit with the changed public sector environment

10.45 It is said that the public sector environment that existed when the Privacy Act was enacted has now changed significantly. The notion, reflected in the State Sector Act 1988, that public sector agencies should work more or less autonomously has now been replaced by an emphasis on collaboration and integrated service delivery.

10.46 The view that the Privacy Act imposes barriers to the sharing of client information when this is necessary to enable government agencies to work together better is highlighted in the Ministry of Social Development's Briefing to the Incoming Minister 2008. In the Organisation Briefing section of the document, under the heading "Working with the Privacy Act", the Ministry states:[770]

> Government agencies often need to work together to achieve the results the government is seeking. This is reflected in the State Services Commissioner's Development Goals for the State Sector which emphasise the importance of networked state services, co-ordinated state agencies and accessible state services.
>
> There are a number of things social services agencies can do better if we could share client information more easily. These include:
>
> - prevent the creation or exacerbation of debt
> - provide more tailored services to joint clients
> - better manage ex-offenders in the community.
>
> We have training in place to ensure our staff understand the Privacy Act, and are able to comply with it. We are also working across agencies to seek practical, non-legislative solutions to barriers wherever we can.

Law enforcement exemptions too narrow

10.47 The scope of the law enforcement information regime in the Act has been raised as an issue, although in some instances this seems to be the result of a misunderstanding of the legislation. There is said to be a lack of clarity for agencies about whether principle 11 allows law enforcement agencies (such as the Police) to share information with agencies that are not regarded as law enforcement agencies but that have law enforcement functions (for example, New Zealand Customs, Ministry of Fisheries, the Commerce Commission, and the Ministry of Economic Development). The specific regime for law enforcement information in Schedule 5 of the Act may also reinforce this distinction, and affect the willingness of non-law enforcement agencies to share information with law enforcement agencies.

---

770 Ministry of Social Development *Briefing to the Incoming Minister: Organisation briefing* (Wellington, 2008) 36. Note that the Development Goals for the State Sector referred to in the Briefing have been discontinued as a separate "brand", but they continue to be reflected in the State Services Commission's objectives for the public sector: State Services Commission "State Services Commission Strategic Direction" www.ssc.govt.nz/strategic-direction (accessed 16 February 2010).

10.48 An example of where a number of government agencies have been able to put in place an information sharing regime as part of an inter-agency initiative is the Priority Offenders Initiative (POI).[771] The core participating agencies involved in the POI are the New Zealand Police, Department of Corrections, the Ministries of Education, Health, Justice, and Social Development (Work and Income and Child Youth and Family) and the New Zealand Housing Corporation. Representatives from these agencies come together in a "multi-agency group" (MAG) in each location in which the POI is being undertaken. Each MAG works together to identify individuals in their community who are aged 17 or older and who frequently come to the attention of the criminal justice system ("priority offenders"). The MAG then takes a collaborative case management approach to assist participants by addressing the social, cultural, and economic factors in their lives that increase their risk of offending. Assistance is also offered to the families of participants.

10.49 The objective is to provide priority offenders with the support and assistance they need and an opportunity to change their offending lifestyle. For priority offenders who continue offending, the idea is that they will be swiftly apprehended and returned to the criminal justice system.

10.50 The POI involves an information sharing protocol developed in consultation with the Privacy Commissioner.[772] A key aspect of this protocol is the division of the initiative into two distinct stages: stage one is the identification and selection of priority offenders as suitable for participation and engagement with them to gain agreement to participate: stage two is the delivery of assistance to the priority offender and his or her family through an intervention plan. Limited information sharing among the participating agencies is permitted for stage one. If a priority offender agrees to participate, and provides informed consent to the sharing of information for the purposes of the initiative, wider information sharing may take place among participating agencies for stage two. Participation by a priority offender's family similarly requires agreement and consent by each family member.

Specific barriers to social services agencies imposed by Privacy Act

10.51 It is said that the Privacy Act creates real barriers to information sharing and interagency co-operation, particularly where social services agencies work together.

10.52 Problems are said to exist in the following three key types of agency activity:

- The Act does not provide clear guidance on when information can be shared. In situations where information exchange is voluntary (no one is statutorily required to provide the information), confusion and risk-averse behaviour results from different levels of staff knowledge of the Act, and different legal interpretations.

771 The Ministry of Justice website contains a detailed description of the POI, together with links to further explanatory material. See www.justice.govt.nz. POI is being trialled for 3 years (2008–2010), and is being monitored and evaluated during this period to assess its effectiveness.

772 This can be found at Ministry of Justice *Priority Offenders Initiative Practice Guide* (Wellington, 2008) Appendix E.

- The information matching regime in the Act can only be accessed through specific legislative authority, and the time and resources required to enact and implement an authority are considerable. The ongoing administration and compliance costs of the information matching regime are also substantial.
- Agencies do not have shared access to information about common clients. This affects the ability of social services agencies to work together more closely to improve outcomes for clients with multiple problems, which impact on each other and are associated with different agencies. An example is clients with debts to more than one agency.

Limitations of information matching regime

10.53 The information matching regime in Part 10 of the Act is a tightly-controlled and highly-structured information sharing regime. Datasets can be compared electronically for a specific purpose. Case-by-case exchanges of information between agencies, which by their nature are less formal and more episodic, fall outside the scope of the regime. Further, information matching programmes allow for the exchange of factual information. Information of a more qualitative nature is not covered by the regime.

Limitations of section 54 exemptions

10.54 Section 54 is designed to provide one-off exemptions from the Privacy Act in special circumstances. It is not intended to provide for routine or ongoing disclosures of information.[773]

Original purpose of collection does not allow use in later initiative

10.55 The purpose for which personal information is collected is established at the time of collection and is intended to give some finality to the purposes for which the information can be used. This indeed is the objective of all data protection legislation. Agencies may find that this purpose does not allow the use of the information in an initiative or programme developed later. Unless a very wide (and perhaps overbroad) purpose is attributed to the information collection, it will be difficult or impossible for agencies to foresee what other purposes an agency may wish to use the information for in the future. A factor possibly unique to the public sector in this context is the impact of changes in government policies over time.

10.56 While these difficulties could be overcome by gaining individual consent to use or disclose the information for a different purpose, the large number of people involved may make this impractical. The time and costs involved may be considerable, and more than one agency may need to seek consent.

773 For further discussion of the scope of this provision, see chapter 5.

Research findings on information sharing between government agencies

10.57 We have not undertaken our own survey of government agencies on the issues raised above with respect to information sharing; that would be too large an undertaking in the context of the current exercise. However, we have had the benefit of access to the findings of a recent research project undertaken in the School of Government of Victoria University of Wellington (VUW). The project, "Improving Information Sharing for Effective Social Outcomes", was commissioned by a group of New Zealand public service chief executives under the Emerging Issues Programme." The report on this project was published at the end of 2009.[774] Its findings are very helpful.

10.58 Because the report is publicly available, we do not propose to rehearse its findings in any detail. It examined five case studies on information sharing practices in a number of inter-agency initiatives. Three of the studies had a public safety mandate, and two had a public service mandate, with public safety also a key issue. Some of the research findings were as follows:

- The configuration of public service agencies affects information sharing. Agencies sometimes have a single, bounded or "siloed" focus rather than a broader "public service" focus.
- Where agencies had a public safety mandate the Privacy Act was not seen as an obstacle. Principle 11 was seen as providing adequate authority to share information.
- In the case of agencies with a public service mandate, there were greater uncertainties as to the application of the Privacy Act. It was not seen as helpful in some cases.
- Overall, there was an awareness among agency staff of the Act's requirements, but sometimes that awareness was not backed up with detailed knowledge.
- Legal interpretations of the Act differ, and there was sometimes uncertainty about whether the Privacy Commissioner would uphold an agency's decision.
- When protocols were developed they were regarded as very helpful. But some were very narrow, and restricted to particular initiatives.
- There was a reluctance to share health information.
- While consent forms were widely used, their content and scope varied considerably from agency to agency.
- Technical issues were important. Some smaller agencies were hampered by lack of technology.
- Professional relationships, mutual trust, and cultural issues were important.
- There was a tendency for participants to rely more on "soft" (that is, unwritten) information than on "hard" written information exchanged through formal channels.

774 Miriam Lips, Rose O'Neill and Elizabeth Eppel *Improving Information Sharing for Effective Social Outcomes* (Victoria University of Wellington, 2009) available at http://e-government.vuw.ac.nz/summary_information_sharing.aspx.

What are the key issues raised?

10.59 Some of the difficulties raised by government agencies go to the heart of the Privacy Act and its principles-based, open-textured, approach. In chapter 2, we expressed our preliminary conclusion that the Act should continue to be based on this approach. The advantages of a flexible approach to privacy outweigh the disadvantages of lack of certainty and predictability that might not be present in a rules-based system of privacy regulation.

10.60 With respect to information matching, our preliminary conclusions on this regime in chapter 9 are that the current regime is appropriate. Given the serious privacy risks arising out of information matching, we think that the strict requirements on the activity in Part 10 and Schedule 4 of the Act are justified and not unnecessarily onerous.

10.61 Some of the issues raised by government agencies also emerge from the VUW research. As the above summary indicates, knowledge of the Act among staff differs as between agencies, and legal interpretations of the Act can also differ. Lack of knowledge and clarity can lead to lack of confidence in decision-making and to risk aversion. A focus on organisational arrangements, rather than broader "public service" common purposes and outcomes, can impede appropriate information sharing.

10.62 Changes in the configuration of the public service over time are not something that, on their own, should affect the ability of agencies to share personal information. Effective and efficient delivery of government services should not be impeded by information sharing provisions that assume particular public sector structures. Moreover, given the scope and breadth of the State's activities, obtaining the consent of individuals who have provided personal information to the use of that information for a different purpose could be inconvenient, particularly where multiple agencies are involved. Efficiency is important for both government and business.

10.63 Unnecessary compliance costs are to be avoided for the State, as much as for the private sector. The costs involved in the diversion of precious public sector resources funded by the taxpayer due to the uncertainties engendered by differing interpretations of the Privacy Act should also not be underestimated.

10.64 There are also costs where agencies seek specific legislative authority for their particular information sharing initiative. While this might ultimately provide them with certainty, the process is resource-intensive, time-consuming, and lengthy. In addition, unlike in the case of information matching, there is currently no authoritative framework for assessing such proposals. There is a danger that proposals are not subject to adequate scrutiny at the policy development stage, that consultation is inadequate, and that Parliament is unable to properly assess such proposals.

10.65 The other side of the coin relates to transparency and accountability in the information sharing activities of public sector agencies. There is a need to provide reassurance to citizens that their personal information is well protected and is not inappropriately shared with other agencies or used for other purposes. The current Act may not provide this level of assurance.

10.66 So, despite our initial conclusion that fundamental and radical changes to the Privacy Act are not justified, we think that the status quo is probably unsatisfactory too. However, we have an open mind on just how significantly the Act needs to be changed to better facilitate appropriate information sharing among government agencies. For this reason, we set out a range of options below for facilitating information sharing arrangements under the Act.

10.67 Before outlining some options for addressing these difficulties in the New Zealand context, we look at developments in this area in a number of comparable overseas jurisdictions.

OVERSEAS APPROACHES

10.68 This section looks at approaches that are in place or have been proposed in a number of jurisdictions similar to New Zealand with respect to data sharing by government agencies. The jurisdictions are the United Kingdom, Canada, Australia and Ireland. It is our assessment that no jurisdiction appears to have come up with a complete solution to the issue of data sharing by government agencies. Indeed, some jurisdictions, such as British Columbia in Canada, are engaged in an exercise similar to our own to identify enhancements to existing data sharing mechanisms that strike an appropriate balance between privacy interests and the efficient and effective conduct of the business of government.

10.69 It is also clear from the experience of the United Kingdom that proposals to facilitate greater data sharing by government agencies can be highly controversial, and politically risky. While the particular circumstances that gave rise to controversy in the United Kingdom are not necessarily applicable to the New Zealand context, they do show that any proposal needs to strike a careful and appropriate balance between privacy and other interests, and be clearly justifiable.

10.70 It is always dangerous to rely too heavily on overseas experience: laws, the understanding of them, and the culture surrounding them, can vary from place to place. It may well be that in some countries privacy values or information "ownership" perceptions are more firmly embedded than in others, and thus lead to different "default positions" or starting points. The New Zealand VUW report makes the point that the New Zealand culture may in some ways be more conducive to sharing: in our small country, officials tend to know each other, and to be able to build trust in their relationships.[775]

775 Miriam Lips, Rose O'Neill and Elizabeth Eppel *Improving Information Sharing for Effective Social Outcomes* (Victoria University of Wellington, 2009) 69. This report contains, in chapter 6, a useful survey of the position in other jurisdictions.

United Kingdom

10.71 In the United Kingdom, as with information matching, the legal framework applying to information sharing consists of the Data Protection Act 1998, other specific legislative provisions,[776] the common law, the European Union Data Protection Directive,[777] and the Human Rights Act 1998 (in particular, the incorporation into UK law of a general right to respect for private and family life under article 8 of the European Convention on Human Rights).

10.72 Within the last decade, a number of reports from various government bodies in the UK have considered the issue of data sharing in the context of improving public services. Lack of clarity in the legal regime relating to data sharing and data protection has been a constant theme.

10.73 In October 2007 the Information Commissioner issued an Information Sharing Framework Code of Practice.[778] The framework code has no legal status, and is principally intended to support good practice in information sharing by assisting organisations to design their own solutions to compliance issues relating to information sharing. Organisations can use it to develop their own codes of practice for sharing information, integrate some or all of its content into existing policies and procedures, or use it as a checklist to evaluate existing policies and procedures.

10.74 In 2007–2008, Richard Thomas and Mark Walport undertook an independent review of the law and policy relating to data sharing in the UK.[779] The terms of reference of the review required the reviewers to consider whether changes were needed to the operation of the Data Protection Act 1998, to provide recommendations on the powers and sanctions available to the Information Commission's Office and the courts in the legislation governing data sharing and data protection, and to provide recommendations on how data-sharing policy should be developed to ensure proper transparency, scrutiny and accountability.

10.75 Echoing earlier studies, the reviewers' conclusion in their final report (the *Data Sharing Review Report*) was that "in the vast majority of cases, the law itself does not provide a barrier to the sharing of personal data. However, the complexity of the law, amplified by a plethora of guidance, leaves those who may wish to share data in a fog of confusion."[780]

776 See examples in UK Parliament's Joint Committee on Human Rights *Data Protection and Human Rights Fourteenth Report of 2007/8* (HL Paper 72, HC 132, London, 2008) Table 1.

777 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

778 Information Commissioner's Office *Framework Code of Practice for Sharing Personal Information* (London, 2007).

779 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008).

780 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) i.

10.76 The *Data Sharing Review Report* includes a number of particularly insightful comments and observations about data sharing that we have found helpful in framing our own thoughts about an appropriate information sharing regime in New Zealand. In summary, the points are as follows:

- the propriety of sharing data needs to be judged on a case by case basis;
- a test of proportionality should be used to determine when sharing of data is appropriate;
- data sharing poses risks that need to be managed; and
- high levels of accountability and transparency are vital to the way organisations handle and share personal information.

10.77 The review made the following key recommendations relating to information sharing:

- There should be a significant improvement in the personal and organisational culture of those who collect, manage, and share personal data.[781] Enhanced training, professional development, accountability, reporting and auditing are needed to improve the handling and sharing of personal information. (In New Zealand we suspect that *significant* improvement may not be needed. But this is not to say that more work is not required.)
- The Information Commissioner should have a statutory duty to publish and periodically update a code of practice relating to information sharing.[782] The Commissioner should also be able to endorse context-specific guidance that elaborates the code.[783]
- There should be a fast-track legislative procedure to enable legal barriers to information sharing (whether statutory or common law) to be removed or modified in appropriate cases, after Parliamentary scrutiny.[784] The Secretary of State, in precisely defined circumstances, should have the power, by Order, to remove or modify restrictions on information sharing by repealing or amending other primary legislation, changing any other rule of law (for example, the application of the common law of confidentiality to defined circumstances), or creating a new power to share information where that power is currently absent. An opinion from the Information Commissioner as to the compatibility of the proposed information sharing arrangement with data protection requirements would be required before a draft Order could be laid before Parliament,[785] and both Houses of Parliament would need to confirm the proposed Order by affirmative resolution before it became law.

10.78 The reviewers noted that the fast-track procedure "would not be appropriate for large-scale data-sharing initiatives that would constitute very significant changes to public policy".[786] Dedicated primary legislation would be more appropriate in those cases.

781 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) i.

782 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) recommendation 7(a).

783 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) recommendation 7(b).

784 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) recommendation 8(a).

785 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) recommendation 8(b).

786 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) para 8.47.

10.79 Other recommendations related to the powers and resources of the Information Commissioner's Office (including additional inspection powers and increased penalties under the Data Protection Act), the use of personal information for research and statistical purposes, and safeguards for personal information held in publicly-available sources.

10.80 The government response to the report endorsed the reviewers' key findings and recommendations.[787] The response noted that the appropriate legislative mechanism to authorise or require a data sharing arrangement needs to be decided on a case-by-case basis: while primary legislation will often be the appropriate vehicle, sometimes a fast-track process may be justified.[788]

10.81 The UK government introduced the Coroners and Justice Bill into the House of Commons on 14 January 2009. Clause 152 of the Bill as introduced proposed to insert a new Part 5A into the Data Protection Act 1998, providing for Ministers of the Crown to make information-sharing orders enabling agencies to share information consisting of or including personal data. A Minister could make an information-sharing order only if satisfied that the sharing of information enabled by the order is necessary to secure a relevant policy objective, that the effect of the provision made by the order is proportionate to that policy objective, and that the provision made by the order strikes a fair balance between the public interest and the interests of any person affected by it.

10.82 Further, an information-sharing order could remove or modify any prohibition or restriction imposed (whether by virtue of an enactment or otherwise) on the sharing of the information or on further or onward disclosure of the information. An order could also, among other things, modify (which includes amend, add to, revoke, or repeal) any enactment. Proposed information-sharing orders would have to be widely publicised, and representations sought and taken into account. A copy of the draft order would have to be provided to the Information Commissioner, who could report his or her opinion on whether or not the order was justified. An information-sharing order could not be made unless a draft of the order was laid before each House of Parliament (or, in the case of Scotland, Wales, or Northern Ireland, the relevant legislative body), and approved by resolution.

10.83 The proposed new Part 5A also required the Information Commissioner to issue a code of practice containing practical guidance in relation to the sharing of personal data in accordance with the requirements of the Data Protection Act, and such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data. Ministerial approval of the code was required, and Parliament could, by resolution, decline to approve the code. A code would not be directly enforceable, but could be taken into account in the context of determining any question arising in any legal proceedings (whether under the Data Protection Act or otherwise) or in the exercise of the Information Commissioner's functions.

787 Ministry of Justice *Response to the Data Sharing Report* (London, 2008).

788 Ministry of Justice *Response to the Data Sharing Report* (London, 2008) 16.

10.84 The Opposition did not support the new provisions,[789] and there was considerable public outcry against the provisions in the Bill to facilitate greater information sharing. In an open letter to the Minister in charge of the Bill, Privacy International and a large number of professional bodies condemned the new powers as a dangerous threat to privacy and called on the removal of the provisions from the Bill.[790]

10.85 The Information Commissioner, having initially welcomed aspects of the Bill, subsequently expressed concerns about the width of the powers in it.[791] He considered that the Bill's information sharing provisions were too wide, and its safeguards relatively weak.[792] He felt that the provisions should only apply in precisely defined circumstances where there is a legal barrier to information sharing and where that information sharing would be in the public interest. An additional safeguard was also needed to prevent the use of information-sharing orders in the context of large-scale data sharing initiatives that would constitute significant changes to public policy.

10.86 The Government subsequently withdrew clause 152[793] when the Bill received its third reading in the House of Commons on 24 March 2009. The provisions relating to a data sharing code of practice remained in the Bill, and were eventually enacted as new sections 52A to 52E of the Data Protection Act 1998.[794]

10.87 It has to be acknowledged that the UK Government's proposal for more expansive powers to authorise information sharing among public sector agencies arose at a time when there had been a number of high-profile data losses by UK public agencies, including HM Revenue and Customs and the Ministry of Defence.[795] This contributed to a lack of public confidence in the ability of government agencies to safeguard personal information against unauthorised disclosure or loss. In addition, the UK Government was promoting other contentious legislation at the same time, including proposals to require telecommunications companies and others to retain data, and build up large databases of personal information.

789 See, for example, the comments of Mr Dominic Grieve (Conservative): "It beggars belief that the Government should be seeking a draconian transformation in our law to enable them to share private data about individuals. Those data will have been collected in confidence for specific purposes but their ability to be shared right across Government will be sanctioned merely by statutory instruments that will be unamendable in this House. The controversial nature of such a proposal cries out for stand-alone legislation, and I can tell the Secretary of State that we will seek to remove it from the Bill." Hansard, House of Commons, 26 January 2009, column 43.

790 Simon Davies, Director, Privacy International and others, to Rt Hn Jack Straw, Secretary of State for Justice (28 February 2009) Open letter. See also Privacy International *Sharing the Misery: The UK's strategy to circumvent data privacy protections* (Black Zone Report Series, 2009).

791 Information Commissioner's Office *Coroners and Justice Bill: Information Commissioner's commentary on the Data Protection Clauses (151–154 & Sch 18)* (London, February 2009).

792 Information Commissioner's Office *Coroners and Justice Bill: Information Commissioner's commentary on the Data Protection Clauses (151–154 & Sch 18)* (London, February 2009) 2.

793 By this stage the clause had been renumbered as clause 154.

794 Coroners and Justice Act 2009 (UK), s 174.

795 For a basic outline of each of these cases see chapter 16, paragraph 16.11.

Canada

Federal

10.88 There is no specific provision in the Canadian Federal Privacy Act relating to information sharing. However, the broadly drafted section 8(2)(m) permits government institutions to disclose personal information, without the consent of the data subject, for any purpose where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or disclosure would clearly benefit the individual to whom the information relates. The head of the government institution must notify the Privacy Commissioner in writing of any disclosure of personal information under that provision prior to the disclosure where reasonably practicable, or in any other case forthwith on the disclosure. The Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to whom the information relates of the disclosure.

Alberta & British Columbia: disclosure for delivery of common or integrated programme, service or activity

10.89 Under the privacy legislation in force in Alberta[796] and British Columbia[797], the collection, use, and disclosure provisions of the legislation generally govern the matter of information sharing. However, the privacy legislation of both provinces permits a public body to disclose personal information to an officer or employee of another public body, or to a Minister, if the disclosure is necessary for the delivery of a common or integrated programme, service or activity and for the performance of the duties of the officer, employee, or Minister to whom the information is disclosed. The legislation does not set out requirements for the establishment of a common or integrated programme or service.

Alberta

10.90 Guidance material issued by the Alberta Access and Privacy Unit of the Ministry of Service Alberta, the government agency responsible for the administration of the Freedom of Information and Protection of Privacy Act, outlines the scope of the "common or integrated programme" provision of the Act.[798] The fact that agencies have clients in common is not, by itself, sufficient to make a programme or service common or integrated. A common programme or service is a single programme or service that is provided or delivered by two or more agencies. An integrated programme or service is a programme or service that has several distinct components, where each component may be provided or delivered by a separate agency, but together the components make up the programme or service.

10.91 Agencies that wish to establish a common or integrated programme or service are advised to consider undertaking a privacy impact assessment as part of the programme proposal and providing the assessment to the Information and Privacy Commissioner for review and comment.

796 Freedom of Information and Protection of Privacy Act RSA 2000 c F-25.

797 Freedom of Information and Protection of Privacy Act RSBC 1996 c 165.

798 Access and Privacy Service Alberta *FOIP Bulletin Number 8, Common or Integrated Programs or Services* (Revised March 2009).

10.92 Agencies that determine that the sharing of personal information is necessary and is authorised by the Act are also advised to do so under a written personal information sharing agreement,[799] which provides a formal mechanism for the efficient and timely sharing of personal information, puts limits on the type and amount of personal information that will be disclosed and the purposes for which it will be used, and provides additional privacy protection, both during and after the sharing, by binding the parties to enforceable terms and conditions.

British Columbia

10.93 In British Columbia, there has been significant pressure in recent years to increase the amount of information sharing between government agencies. There has been considerable investment in information technology infrastructure in that province, accompanied by calls to utilise that infrastructure to improve the delivery of government services to citizens.

10.94 The British Columbia Premier's Technology Council[800] has highlighted the issue in a number of its reports. In its most recent report, the Council stated:[801]

> In the past, government program delivery has been the responsibility of each discrete Ministry. The focus has traditionally been on each individual program and how best to deliver it. The advent of modern information management technology allows for a new model, commonly referred to as Citizen Centred Services. It requires government to focus on the citizen rather than the program.
>
> A key to success is information sharing. Responsible sharing of information enhances the services that the BC government can provide and generates significant benefit for citizens. It allows government and its service providers to accurately ascertain the needs of the citizen and then meet those needs rapidly and efficiently. It quickly informs citizens of those government services in which they are most likely to be interested.

10.95 The Office of the Chief Information Officer (OCIO)[802] in British Columbia is responsible for the British Columbia legislation governing the protection of privacy and personal information. The Knowledge and Information Services Branch of the OCIO, among other things, "supports efforts to integrate policy analysis across government and to build cross government relationships necessary for information, research and data sharing. [It] is leading the development of an information sharing framework between government and agencies."[803]

---

799 Access and Privacy Service Alberta *Guide for Developing Personal Information Sharing Agreements* (Revised October 2003) 2.

800 The Council was formed in 2001, and is comprised of up to 25 members from the private sector and academia. The mandate of the council is to provide advice to the Premier on all technology-related issues facing British Columbia and its citizens. See further www.gov.bc.ca/premier/technology_council.

801 Premier's Technology Council *12th Report* (Vancouver, April 2009) 24–25.

802 The Office of Chief Information Officer is part of British Columbia's Ministry of Labour and Citizens' Services.

803 "Knowledge and Information Services Branch" www.cio.gov.bc.ca (accessed 17 February 2010).

10.96 The 2008–2009 Annual Report of the Office of the Information and Privacy Commissioner for British Columbia notes that the British Columbia Government has recently initiated a number of programs that depend on facilitating interagency sharing, justified by reference to improving service delivery and efficiencies. The Commissioner indicated that he was actively monitoring and providing comment on these initiatives to ensure that existing privacy law is complied with and that they meet reasonable privacy expectations. The Commissioner's office is working on a position paper on the disclosure of personal information within and across government. In the Commissioner's view, the British Columbia government should initiate public consultation by publishing a position paper, followed by meaningful and extensive stakeholder consultations.[804]

Australia

Federal

Privacy Act

10.97 At the Federal level in Australia, the Privacy Act 1988 (Cth) does not make specific provision for information sharing between public sector agencies. Whether or not agencies can share information is determined in accordance with the Information Privacy Principles (the principles which apply to the public sector) and exceptions.

10.98 However, the Act does empower the Privacy Commissioner to make public interest determinations (PIDs) under Part VI of the Act, which lie somewhere between the New Zealand section 54 exemptions and codes of practice. A PID is a determination that an act or practice of an agency or organisation, which would otherwise breach an Information Privacy Principle, National Privacy Principle, or an approved privacy code, is to be regarded as not breaching the principle or code. The Commissioner must be satisfied that the public interest in the agency doing the act, or engaging in the practice, outweighs to a substantial degree the public interest in adhering to the relevant principle or code.

10.99 The ALRC's review of the Act included a number of recommendations directed at achieving greater transparency in information-sharing arrangements. In particular, it noted the public interest in the public, where appropriate, knowing how agencies share personal information. It therefore recommended that agencies that are required or authorised by legislation or a PID to share personal information, should develop and publish documentation that addresses the sharing of personal information, and publish other documents (including memoranda of understanding and ministerial agreements) relating to the sharing of personal information.[805] The Australian Government has not yet responded to this recommendation.

804 Office of the Information and Privacy Commissioner for British Columbia *2008–2009 Annual Report* (Vancouver, 2009) 8–9.

805 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2009) recommendation 14 – 1.

10.100 The ALRC also suggested that the Office of Privacy Commissioner should consider including some additional matters in its existing guidance material on the Act. For example, the guidance could explain: how the privacy principles operate to allow or prevent the sharing of information in certain circumstances; when a public interest determination, a temporary public interest determination or a code will be appropriate; when a privacy impact assessment should be prepared; and the development of memoranda of understanding and protocols in relation to information-sharing schemes.[806]

National Government Information Sharing Strategy

10.101 The Australian Government has recently adopted a National Government Information Sharing Strategy (NGISS).[807] It was endorsed by the Council of Australian Governments' (COAG) Online and Communications Council on 12 December 2008.[808] The strategy notes:[809]

> Gaining benefits from sharing information across all levels of Australian governments is a complex objective that can only be achieved with a consistent national approach. A National Government Information Sharing Strategy (NGISS) will identify the best practices, tools and further requirements for success and provide the foundation for future development.

The strategy states a vision for information sharing as follows: "Timely, reliable, and appropriate information sharing is the foundation for good government and has the capacity to deliver a better way of life for all Australians."[810]

10.102 The strategy notes that background research as part of the development of the strategy identified certain barriers preventing information sharing:[811]

- A lack of leadership within agencies: "competing agenda and differing goals across, and within, the three tiers of government make it difficult to gain cohesive support for information sharing from public sector leaders".
- The absence of a clear value proposition: the usefulness of information gathered by one agency to another part of the same agency, or other agencies or jurisdictions, is not recognised; excessive cost-recovery policies can inhibit re-use of information; or information and its associated intellectual property is undervalued and shared too freely.

---

806 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2009) para 14.54.

807 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009).

808 Online and Communications Council *Sixteenth Online and Communications Council Communiqué* (December 2008). See also Andrew Jones, South Australian Office of the Chief Information Officer *National Government Information Sharing Strategy* (May 2009) Power point presentation.

809 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009) 2.

810 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009) 5.

811 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009) 7.

- Information management practices that restrict sharing capability: inconsistent application of interoperability frameworks, lack of a common approach to information management, and lack of whole-of-government training in information management.
- Privacy and accountability concerns: "the complexity of privacy laws often results in the default response to requests for information (that might be considered sensitive) as: 'we cannot share our information because of privacy laws.' This response is often given instead of determining (through the appropriate channels) whether the information can, in fact, be shared.".
- A culture that is resistant to sharing information: "there is still a culture of 'information is power' that results in the defensive protection of an organisation's information assets." Knowledge management practices are poorly defined and applied. There is also a generational divide in attitudes to information sharing, with the ready availability and easy sharing of information familiar to the younger generation (for example, through social network sites) being something that the older generation has not experienced or adopted.

10.103 The following principles for information sharing form the basis for the strategy:[812]

- provide leadership;
- demonstrate value;
- act collaboratively;
- establish clear governance;
- establish custodianship guidelines;
- build for interoperability;
- use standards-based information;
- promote information re-use; and
- ensure privacy and security.

10.104 Particularly relevant to the issues in this chapter is the emphasis that the strategy places on agencies acting collaboratively. The strategy states:[813]

> Australian governments can no longer sustain agencies operating in silos. A new culture of collaboration is required. Custodians of public sector information need to shift to finding reasons why they must and can share information.
>
> Governments must act collaboratively, but also need to take into account privacy, confidentiality and security requirements, as well as maintaining appropriate accountability of the custodians of the information assets. A better understanding of these issues and how to overcome them will lead to governments remaining compliant with legislative requirements, while being flexible enough to meet the changing needs of the Australian community.

812 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009) 6.

813 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009) 18.

10.105 The strategy emphasises the importance of clear and appropriate governance arrangements for information sharing, with the need for information custodians "to develop a clear understanding of the privacy framework and use this knowledge as a tool in overcoming the perception that privacy is a barrier."[814] Transparency is also highlighted, with the strategy emphasising that "governments must be able to demonstrate to the Australian public that the relevant protections are in place, the privacy laws are being met, and that the process of sharing is covered by transparent and publicly-available guidelines."[815]

10.106 The NGISS is to be followed by an implementation plan to identify and report on progress across all jurisdictions. At the date of writing, the implementation plan had yet to be published. However, the NGISS identifies a number of initiatives that are already in place to support the strategy, such as a National Collaboration Framework, an Information Interoperability Framework, and a collaborative workspace for government agencies (GovDex).[816] No specific legislative initiatives with respect to privacy are outlined in the strategy.

States

10.107 In New South Wales, neither the Privacy and Personal Information Protection Act 1998 nor the Health Records and Information Privacy Act 2002 contains special provision for information sharing by public sector agencies. However, both Acts provide for the issuing of codes of practice that modify the application of the information protection principles or, as the case requires, the health privacy principles. In addition, both Acts empower the Privacy Commissioner to make a direction exempting an agency from complying with an information protection principle or health privacy principle, as the case requires, or with a code of practice, or modifying the application of a principle or code to an agency. In each case the making of a direction requires the approval of the relevant Minister, and the process may involve some consultation with affected parties. Several directions have been made to authorise the exchange of personal information among public sector agencies and NGOs involved in multi-agency initiatives with respect to the care and protection of children and young persons.

10.108 The Northern Territory Information Act 2002 provides for both codes of practice that modify an information privacy principle in relation to a public sector organisation, and authorisations that exempt public sector organisations from compliance with certain principles. Under section 81, the Information Commissioner, on the application of a public sector organisation, may authorise the organisation to collect, use or disclose personal information in a manner that would otherwise contravene or be inconsistent with the Information Privacy Principles relating to the collection, use, or disclosure of personal information, or sensitive information. Unlike the Federal Privacy Act and the NSW Privacy and Personal Information Protection Act, there are two limbs to the test for determining

814 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009) 19.

815 Australian Government, Department of Finance and Deregulation *National Government Information Sharing Strategy: Unlocking Government information assets to benefit the broader community* (Canberra, August 2009) 25.

816 See www.finance.gov.au for information about these initiatives.

whether the Commissioner can grant an authorisation. The Commissioner must be satisfied both that the public interest in collecting, using or disclosing the information outweighs *to a substantial degree* the interference with the privacy of persons that might result from collecting, using or disclosing the information; and that the benefit to persons of collecting, using or disclosing the information outweighs the interference with the privacy of those persons that might result from collecting, using or disclosing the information.

10.109 The Queensland Information Privacy Act 2009 provides for the Information Commissioner to issue an approval waiving or modifying an agency's obligation to comply with an information privacy principle, either temporarily or indefinitely.[817] The Commissioner can issue an approval only if the Commissioner is satisfied that the public interest in the agency's compliance with the privacy principles is outweighed by the public interest in waiving or modifying the agency's compliance with the privacy principles to the extent stated in the approval.

10.110 Under the Tasmanian Personal Information Protection Act 2004, the Minister responsible for the administration of the Act may grant an exemption from compliance with any or all provisions of the Act if the Minister is satisfied that the public benefit outweighs *to a substantial degree* the public benefit from compliance with the personal information protection principles.

10.111 Western Australia does not have specific privacy legislation. An Information Privacy Bill was introduced into the Western Australian Parliament by the previous government in 2007,[818] and passed by the Legislative Assembly.[819] It received a second reading in the Legislative Council that same year, but has not subsequently progressed. The current government has indicated that it plans to proceed with the Bill.[820]

10.112 Part 6 of the Bill provides for the exchange of personal and health information between government agencies, and (with the approval of a Privacy and Information Commissioner) between government agencies and persons or bodies in the private sector. The provisions are intended to implement key recommendations of the Gordon Inquiry in 2002.[821] That inquiry found that legislative and policy changes were necessary for the effective coordination of service provision to Aboriginal communities, particularly in relation to the sharing of confidential information. The inquiry recommended that the required legislative changes be progressed as a matter of urgency.

10.113 The circumstances in which personal and health information may be exchanged under Part 6 are essentially where the disclosure is for the purpose for which the information was collected, or where the disclosure falls within certain specified exceptions to the Information Privacy Principles and Health Privacy Principles relating to the use and disclosure of information. These exceptions include:

817 Information Privacy Act 2009 (Qld), s 157.

818 Information Privacy Bill 2007, no 193 – 1.

819 (27 November 2007) WAPD (LA) 7839.

820 Reply by CJ Barnett, Premier of Western Australia, to Question without Notice (9 April 2009) WAPD (LA) 3144b.

821 Sue Gordon *Putting the picture together, Inquiry into Response by Government Agencies to Complaints of Family Violence and Child Abuse in Aboriginal Communities* (State Law Publisher, Western Australia, 2002).

disclosure to lessen or prevent a serious threat to an individual's life, or to an individual's or public health, to an individual's or public safety, or to an individual's or public welfare; to safeguard or promote the wellbeing of a child or group of children; for law enforcement; for the performance of the licensing functions of a licensing agency; and for the purposes of health research in the public interest. A key feature of Part 6 is that disclosures authorised by or under that Part may take place notwithstanding any statutory confidentiality or secrecy provisions.

Ireland

10.114 In Ireland, a 2008 report on transforming public services noted that:[822]

> if the Public Service is to serve the citizen better through more targeted services and by reducing the administrative burden they experience, the Public Service must be empowered to share and re-use the significant amount of data at its disposal. There are legitimate concerns about the use and security of personally and commercially sensitive data and new legislative and procedural protections are needed to allay these. The ability of the Public Service to harvest the potential of e-government and shared services will be dramatically enhanced if we can make progress in this area.

10.115 The report recommended that:[823]

> Legislative change should be made to empower public service organisations to increase the sharing of information with each other. Consideration should be given to imposing a statutory duty on public bodies to share information except in defined circumstances.

At the date of writing, no legislation appears to have been introduced to give effect to this recommendation.

SOME GUIDING PRINCIPLES

10.116 From our (albeit limited) survey of similar jurisdictions overseas, it is clear that a number of them are grappling with similar issues with respect to the sharing of information among public sector agencies. Where barriers to greater data sharing have been identified, these tend to reflect the findings of the VUW research in New Zealand that the barriers are often organisational and cultural as much as legal.

10.117 The Thomas and Walport Report in the UK makes some observations which we have found helpful in framing our own thoughts. The first point is that the propriety of sharing information needs to be judged on a case-by-case basis. The report says:[824]

> It is impossible to take a generic view of data sharing. Data sharing in and of itself is neither good nor bad. There are symmetrical risks associated with data sharing – in some circumstances it may cause harm to share data, but in other circumstances harm may be caused by a failure to share data. Data sharing needs to be examined in specific terms. Is the sharing of particular elements of personal information for a defined purpose in a precise fashion, likely to bring benefits that outweigh significantly any potential harm that might be associated with the sharing?

822 Government of Ireland *Transforming public services: citizen centred – performance based: Report of the Task Force on the Public Service* (Dublin, 2008) 14.

823 Government of Ireland *Transforming public services: citizen centred – performance based: Report of the Task Force on the Public Service* (Dublin, 2008) 15.

824 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) i.

There are two key steps in the implementation of any scheme to share personal data. The first is to decide whether it is appropriate to share personal data for a particular purpose. The second is to determine how data should be shared, in particular what and how much data, and by what means.

There can be no formulaic answer as to whether or not it is appropriate to share personal information.

10.118 The second point relates to the test for determining when sharing of data is appropriate. The report puts forward the proportionality test. This is defined as:[825]

> the application of objective judgement as to whether the benefits outweigh the risks, using what some might call the test of reasonableness or common sense. Proportionality involves making a considered and high-quality decision based on the circumstances of the case, including the consequence of not sharing. Decisions must flow especially from the principles of relevance and necessity and the need to avoid an excessive approach.

10.119 The third point is that data sharing poses risk:[826]

> When organisations share personal information, they must pay particular attention to these inherent risks: perpetuating or exaggerating inaccurate or outdated data; mismatching data; losing data; and intruding excessively into private lives. This becomes even more critical when entire databases are shared.

10.120 The last points relate to the responsibility of agencies that share data. Here, accountability and transparency are particularly important: "High levels of accountability and transparency are vital to the way organisations handle and share personal information, yet these are all too often absent."[827]

10.121 Transparency also facilitates oversight and reporting. In this respect the detailed reporting and oversight requirements for information matching in the Privacy Act can be contrasted with the absence of such requirements with respect to information sharing.

10.122 It is also important to ensure that facilitating and encouraging greater data sharing does not produce an extreme result at the opposite end of the spectrum from the current cautious and protective approach. A lax and careless approach to the handling of personal information by government agencies is not a desirable or intended outcome either.

10.123 We have been guided by the above principles of specificity, proportionality, risk management, accountability, and transparency in formulating the options for reform set out below.

Q121 Are the principles set out in paragraphs 10.116–10.123 useful in framing a way forward for information sharing? Do you have any other suggestions?

825 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) para 2.8.

826 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) 53.

827 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) para 7.

OPTIONS FOR REFORM

10.124 We proceed now to examine what reforms might be made to facilitate information sharing. The VUW report, referred to above, has made suggestions for improvement. Some of these involve legal matters, but many are of a practical and administrative character, such as ensuring facilitative leadership, the possibility of co-location for partner agencies, provision of training, and the use of secure shared workspaces. The report endorses strongly the adoption of specific information sharing protocols. We support the suggestions in that report. In this issues paper we are concerned with reforms of a legal, or law-related, character. The VUW report concludes that "there is a clear need for legal support of information sharing in the area of providing social services."[828]

10.125 The options we put forward here are:

- Privacy Commissioner guidelines;
- a code of practice;
- a national information sharing strategy;
- treating the public sector as a single entity;
- binding rulings on compliance with the Privacy Act;
- a framework for developing specific legislative authorities;
- transparency and accountability requirements;
- the addition of a new exception to principle 11;
- an extension of the current section 54 exemption power;
- a schedule of authorised data sharing activities;
- a new regime similar to the existing information matching regime; and
- a "common or integrated programme or service" exception.

10.126 These options are not mutually exclusive. Some will require legislative amendment, others will not. Moreover, none of them will provide a conclusive answer. Too often when information sharing is considered the privacy implications seem not to be well understood, and the very issue of privacy is perceived as a barrier. So, regardless of what mechanism is implemented, concerns will remain unless public sector personnel acquire a good understanding of the Privacy Act.

10.127 It would be possible to run some of the new information sharing options as pilot programmes, so that authority for them expires after a few years, and a review of the effectiveness of the programmes is then carried out. Precedents for this in other contexts are the Community Mediation Service (Pilot Project) Act 1983,[829] and the new powers for access to the Motor Vehicle Register introduced by the 2009 amendment to the Land Transport Act 1998.[830]

828 Miriam Lips, Rose O'Neill and Elizabeth Eppel *Improving Information Sharing for Effective Social Outcomes* (Victoria University of Wellington, 2009) 79.

829 The purpose of this Act was to facilitate the establishment and operation of a pilot project in Christchurch, New Zealand, for the provision of mediation. Among other things, the Act conferred privilege on communications made in the course of a mediation session, imposed criminal liability on people breaching the confidentiality of mediation sessions, and conferred protection from civil and criminal liability on mediators in connection with a mediation. The Act expired after 4 years.

830 Land Transport Act 1998, s 241, as amended in 2009.

Guidelines

10.128 Guidance material issued by the Privacy Commissioner, unlike codes of practice, has no formal legal status. However, it is prepared by experts in the field of privacy, and would be expected to provide some level of comfort to those who follow its advice that their actions would not subsequently be found to contravene the Act. As we discussed in chapter 2, the Privacy Commissioner has already issued very useful guidance material on a number of issues.

10.129 Because of the range of activities covered by the public sector, general information sharing guidelines for public sector agencies would probably need to be stated at a reasonably high level. Agencies would then need to tailor this for their own activities and provide more detailed guidance to their staff. Examples of this already exist, such as guidelines developed by the Ministry of Justice in relation to Youth Offending Team meetings,[831] and the interagency information sharing guidelines developed by Child, Youth and Family for organisations involved in the care and protection of children.[832] The latter document contains good examples of likely situations where information may be requested, and guidance on whether or not it can be shared.

10.130 As noted above, the UK Information Commissioner issued an Information Sharing Framework Code of Practice in 2007.[833] New provisions of the Data Protection Act 1998, inserted by the Coroners and Justice Act 2009, require the Information Commissioner to issue a data sharing code of practice, which would not be legally enforceable but could be taken into account in proceedings arising under the Act.[834]

10.131 A component of any information sharing guidelines issued by the Privacy Commissioner that agencies might find particularly useful would be advice to agencies on the development and implementation of information sharing protocols. A number of agencies already have such protocols in place with respect to particular data sharing initiatives with other agencies. The research on information sharing undertaken as part of the VUW project identified the usefulness of protocols for agency staff.[835] An example is the New Zealand Police Family Violence Information Sharing Protocol, dealing with information sharing in the family violence context between such agencies as the Police, Victim Support, women's refuges, and Child, Youth and Family.[836]

831 See www.justice.govt.nz/policy-and-consultation/youth/youth-offending-strategy.

832 Child Youth and Family *Information Sharing Guidelines for Organisations involved in the Care and Protection of Children* (Wellington).

833 See above, para 10.73. Although called a code of practice, the Framework Code has no legal status under the Data Protection Act 1998 (UK).

834 See above, para 10.86.

835 Miriam Lips, Rose O'Neill and Elizabeth Eppel *Improving Information Sharing for Effective Social Outcomes* (Victoria University of Wellington, 2009) 64.

836 New Zealand Police *Family Violence Sharing Protocol* (Wellington, 2006).

10.132 Another useful component of any information sharing guidelines might be a self-assessment mechanism for agencies to use to determine whether or not what they want to do is permitted by the Privacy Act. This might help to promote understanding of the Act and increase consistency of practice. It is, of course, not only the Privacy Commissioner who might issue guidelines. Sometimes an industry group can provide well-informed guidance. For example, the Mental Health Commission took a leading role in respect of guidance on mental health information, with some expert assistance from the Office of the Privacy Commissioner. Much depends on the type of guidance required. The Privacy Commissioner is expert in interpreting the privacy principles, but expertise in other areas may be possessed by others. The purpose for which the guidance is required is also relevant. Sometimes another organisation – the State Services Commission, for instance – may be able to take a more active stance on the desirability of disclosing information in a particular context.

Code of practice

10.133 Codes of practice are examined in detail in chapter 7. Unlike guidelines, codes of practice have legal status under the Privacy Act and are enforceable through the complaints procedure in the Act and the Human Rights Review Tribunal. A code of practice may modify the application of the privacy principles (for example, by prescribing more stringent or less stringent standards, or by exempting actions) or may prescribe how the privacy principles are to be complied with. An example might be a code which amended principle 11 to allow further exemptions from non-disclosure. The VUW report suggests a code of practice for welfare.[837]

10.134 The fact that compliance with the provisions of a code of practice is taken to be compliance with the requirements of the Privacy Act means that a code of practice relating to information sharing would provide a greater level of comfort for public sector agencies that their sharing activities were authorised. However, as with guidelines, a generic code of practice for public sector information sharing might need to be stated at such a high level that it would not provide agencies with sufficient guidance with respect to their particular activities.

10.135 "Local" protocols can provide a good level of agency-specific guidance. One particular advantage of a data sharing code of practice is that it could require data sharing undertaken under it to be covered by information sharing protocols. A code might require these protocols to be approved by the Privacy Commissioner before being implemented, and reviewed at regular intervals to ensure continued relevance.

837 Miriam Lips, Rose O'Neill and Elizabeth Eppel *Improving Information Sharing for Effective Social Outcomes* (Victoria University of Wellington, 2009) 80.

National strategy on information sharing

10.136 The Australian Government's National Government Information Sharing Strategy (NGISS) is outlined above.[838] The NGISS has no legislative backing, but is intended to provide an overarching framework, supplemented by a detailed implementation plan.

10.137 The New Zealand Government could adopt a similar approach. The principal rationale for a national strategy would be to provide official endorsement of appropriate information sharing and encourage a cultural and institutional change on the part of public agencies and individual officials. A strategy could also reinforce the need for agencies to plan their data collection activities with information sharing in mind, so that the purpose of the collection, and the scope of any subject consent to disclosure of the information, are not unnecessarily constraining. A high-level national strategy could be supplemented by more detailed guidance from the Privacy Commissioner in the form of guidelines, as suggested above.

10.138 There are legislative precedents for national policy statements and national strategies. For example, section 45 of the Resource Management Act 1991 provides for the promulgation of ministerial national policy statements. The purpose of a national policy statement is to state objectives and policies for matters of national significance that are relevant to achieving the purpose of the Act. Section 8 of the New Zealand Public Health and Disability Act 2000 requires the relevant Minister to determine a New Zealand health strategy, to provide the framework for the Government's overall direction of the health sector in improving the health of people and communities. Section 8 of the Act also requires the relevant Minister to determine a New Zealand disability strategy, to provide the framework for the Government's overall direction of the disability sector in improving disability support services.

10.139 A New Zealand information sharing strategy could be recognised or required by legislation, but need not be. One "soft" legislative option would be to require the Privacy Commissioner to have regard to the strategy in deciding whether or not information sharing between agencies was allowed. This might therefore supplement the broad obligation on the Privacy Commissioner under section 14(a) to have regard to the right of government to achieve its objectives in an efficient way.

10.140 A question to be considered is whether a national strategy would be too general and high-level to be of real use to agencies in their own fact-specific circumstances. As we noted earlier, it is not possible to take a generic view of data-sharing. Moreover, such a strategy might suggest that there is a sharing route outside the Privacy Act, whereas in reality the Act itself should be the strategy.

838 Paragraphs 10.101–10.106.

Treating the public sector as a single entity for "purpose" provisions

10.141 We wonder whether, and if so how, it might be possible to encourage government agencies to take a whole-of-government view – a "joined-up government" view, as the VUW report puts it – rather than the "siloed" view which is often prevalent now.

10.142 A key fundamental underlying the Privacy Act is the purpose for which personal information is collected or obtained, retained, disclosed, and used. There is reference to purpose in many of the privacy principles. In particular, principle 10 provides that an agency that holds personal information that was obtained in connection with one purpose shall not use it for any other purpose. Principle 11 provides that an agency must not disclose personal information unless it believes, among other things, that the disclosure is a purpose for which the information was obtained, or a directly related purpose.

10.143 How the concept of purpose is perceived and interpreted by public sector agencies and the Privacy Commissioner can therefore be expected to have a significant bearing on data sharing. The VUW report observed that the purpose for which personal information was obtained tended to be aligned with a "siloed" view of organisations, rather than a broader "public service" view of organisational arrangements. If the purpose for which personal information was obtained was aligned with a common purpose and a common outcome among agencies, then greater information sharing would become possible.

10.144 A further and related issue concerns the constraints that the original purpose of the collection of personal information by a public sector agency place on the use of the information in a programme or initiative that another agency wants to implement later on. A narrow, agency-specific view of the function or activity for which the information was originally collected might be expected to work against subsequent sharing of the information with another agency.

10.145 As we have noted, principle 11 allows disclosure where it is "one of the purposes in connection with which the information was obtained" or is "directly related to" those purposes. One way of addressing the issue might be to encourage public sector agencies, by guidelines or otherwise, when collecting information, to state the purpose for which the information is being collected in broad terms so that the purpose does not prejudice the ability to cooperate with other agencies in programmes for the benefit of the individual concerned. Another might be to amend the Privacy Act to provide that, with regard to public sector agencies – and this term may need to be specifically defined for this purpose – there is a presumption that information can be disclosed to other agencies to achieve a purpose which is beneficial to the individual, and is broadly similar to the purpose for which the information was collected or obtained by the agency in question. That presumption might be rebutted by a clear statement at the time of the collection of the information that the information would only be used by the collecting agency, or in cases where sharing would be contrary to the reasonable expectations of the subject.

10.146 However, any such presumption would need to be carefully defined to avoid the impression that personal information provided to one public sector agency automatically meant that it was available across the board to all other public sector agencies.

10.147 Concern could easily be generated that such a provision would be open to abuse, and its very existence could reduce the confidence of members of the public. Some of the more structured options presented later in this chapter might serve the same end, but with more effective safeguards.

10.148 We are not aware of any legislative precedent for a provision of this kind.

Power for Privacy Commissioner to make binding rulings

10.149 The principles-based, open-textured approach of the Privacy Act carries with it the disadvantages of lack of certainty and predictability that might not be present in a rules-based system of privacy regulation. Guidance material provided by the Privacy Commissioner, and the availability of OPC staff to work through proposed data sharing initiatives with public sector agencies, while very helpful, cannot provide agencies with definitive rulings on whether what they propose will or will not comply with the Act. Definitive rulings can currently occur only in subsequent proceedings before the Human Rights Review Tribunal.

10.150 In these circumstances, a risk-averse approach on the part of public sector agencies would stop a data sharing proposal from proceeding in any case where there is doubt about its compliance. Further, the VUW research noted that difficulties arose where agency staff were faced with conflicting legal opinions on what the Privacy Act permitted and did not permit.

10.151 One way of providing greater certainty to public sector agencies with respect to compliance with the privacy principles would be to provide for the Privacy Commissioner to issue binding rulings (also called advance rulings). A binding ruling would constitute an authoritative statement that a particular course of action complies or does not comply with the Privacy Act. Where agencies proposed to undertake data sharing for the purposes of a particular initiative or programme, and there was real doubt about whether data sharing in those circumstances would comply with the Act, the agencies could obtain a ruling on the matter before deciding whether to proceed. A favourable ruling would allow the agencies to proceed in the knowledge that reliance on the ruling (and any conditions specified in it) would be a good defence to any subsequent complaint of a breach of the Act.

10.152 The idea of advance rulings has been canvassed before. In 1997, the then Privacy Commissioner raised the issue of "advance rulings" in a discussion paper for his review of the Privacy Act.[839] The Commissioner indicated that his position was that it was not desirable to make advance rulings as it would interfere with the Commissioner's independent role in relation to the investigation of complaints if there were subsequently to be a complaint. He also stated that it was most likely

839 Office of the Privacy Commissioner *Review of the Privacy Act 1993: Compliance and Administrative Costs* (Discussion Paper 9, Wellington, 1997) 17–18.

that rulings would be sought in borderline cases or where a privacy-friendly or cautious approach was not being adopted, and that these were the very cases in which the Commissioner would be least willing to give a clearance.

10.153 The Commissioner also noted the resource implications of a power to make advance rulings. Full information would be needed from an applicant, and extensive information gathering and, in some cases, expert advice would be necessary to enable the Commissioner to make a ruling.

10.154 The discussion paper asked whether advance rulings would help reduce compliance costs. To the extent that submissions responded to this question, there were mixed views on whether or not advance rulings would be useful or worthwhile. The view of the Ministry of Justice was that there would be little to gain from creating a general function of advance ruling, given the disadvantages identified by the Privacy Commissioner and the existing alternative means of providing guidance and advice.[840]

10.155 Given this feedback, it is perhaps unsurprising that the Privacy Commissioner did not recommend, in *Necessary and Desirable*, the creation of an advance ruling function. Nevertheless, in the light of subsequent experience with the Act, we think that it is appropriate to again consider whether advance rulings would be useful or worthwhile.

Existing provisions for binding rulings in other legislation

10.156 A number of New Zealand enactments provide for advance rulings. The best known is the power conferred on the Commissioner of Inland Revenue to issue binding rulings under the Tax Administration Act 1994 on how the Inland Revenue Department (IRD) will apply tax laws to a particular arrangement. Taxpayers are not required to follow a ruling, but if they do then IRD must apply the tax law in accordance with the ruling.

10.157 The binding rulings system in the context of New Zealand tax laws is currently the subject of an issues paper published by the IRD.[841] The issues paper focuses on concerns with the current system that may require clarification or refinement.

10.158 Of course, there would be differences between taxation binding rulings and privacy binding rulings in that citizens seek the former, whereas state agencies would be applicants for the latter.

10.159 Other enactments that make provision for binding rulings are the Customs and Excise Act 1996,[842] the Climate Change Response Act 2002,[843] and the Building Act 2004.[844]

840 Ministry of Justice submission, December 1997, in Office of the Privacy Commissioner *Review of the Privacy Act 1993: Compliance Cost Submissions* (Auckland, 1998).

841 Inland Revenue Department *The binding rulings system: legislative issues – an officials' issues paper* (Wellington, 2009).

842 Customs and Excise Act 1996, Part 9.

843 Climate Change Response Act 2002, ss 107–117.

844 Building Act 2004, ss 176–190.

10.160 Some years ago, consideration was given to making provision for binding rulings in the context of securities law. In 2000, the Securities Commission published a discussion paper on binding rulings in securities law.[845] The Securities Commission's Annual Report for 2001 notes that, although a number of submissions were in favour of some form of binding rulings power, strong arguments of principle were raised against it.[846] As a result, the Commission decided not to develop a proposal for a binding rulings power, but instead to consider the extent of its existing power to grant exemptions in case of doubt.

Other jurisdictions

10.161 Advance or binding rulings are not a feature of privacy legislation in other jurisdictions. However, the former Information and Privacy Commissioner for British Columbia has suggested that the power to make advance rulings would be useful in providing certainty and predictability in privacy law.[847]

Why is the power to grant exemptions under section 54 insufficient?

10.162 Section 54 of the Privacy Act empowers the Privacy Commissioner to exempt certain activities from compliance with certain privacy principles.[848] The Commissioner can authorise an agency to collect, use, or disclose personal information, even though this would otherwise breach principles 2, 10 or 11, if the Commissioner is satisfied, in the special circumstances of the case, that the public interest outweighs any interference with the privacy of the individual that could result, or that there is a clear benefit to the individual concerned that outweighs any such interference.

10.163 While authority to share data could be sought by public sector agencies under section 54, the provision is of limited usefulness in this context. For one thing, as currently applied by the Privacy Commissioner, section 54 permits the granting of one-off exemptions, rather than generic or ongoing exemptions. A section 54 exemption is therefore unlikely to be of assistance in the context of ongoing public sector initiatives or programmes that require data sharing.

10.164 Further, as the Securities Commission pointed out in its discussion paper on binding rulings, exemptions are not always the most appropriate method for resolving ambiguity or other difficulties of legal interpretation.[849] While exemptions do provide certainty, they have the effect of adapting the law that would otherwise apply to the situation. Binding rulings provide certainty by giving a definitive interpretation on how or whether the law applies to a situation.

---

845 Securities Commission *Binding Rulings on Securities Law: A Discussion Paper (*Wellington, 2000).

846 Securities Commission *Annual Report of the Securities Commission* (Wellington, 2001).

847 David Loukidelis "Enforcing Private Sector Privacy – One Regulator's Perspective" (paper presented to The Frontiers of Privacy & Security – New Challenges for New Century, Victoria, BC, February 2003).

848 For further discussion of section 54, see chapter 5.

849 Securities Commission *Binding Rulings on Securities Law: A Discussion Paper (*Wellington, 2000) paras 8.7–8.9. See also Ministry of Economic Development *Review of Financial Products and Providers: Supervision of Issuers* (Wellington, 2006) para 52.

10.165 In addition, an exemption could create further uncertainty rather than resolve it.[850] The granting of an exemption in a situation where the application of the law is unclear could create the impression for others that the law prevents the action permitted by the exemption. The doubt created might mean that those not covered by the exemption would be prevented from doing what the exemption permits, or would have to apply for an exemption themselves. A binding ruling enables the position to be clarified for everyone.

The arguments against a binding ruling power

10.166 It is a basic constitutional principle that it is the role of the courts to make authoritative rulings on what the law is. However, the Privacy Act works in a different way from ordinary laws. The privacy principles do not, for the most part, confer legal rights, and interpretation and application of the principles are generally undertaken by the Privacy Commissioner through the complaints process and, in a limited number of cases, the Human Rights Review Tribunal. It is almost a closed system, in which the courts very rarely get to rule on the interpretation of the Act. In any event, the compliance and enforcement mechanisms in the Privacy Act are intended to provide a low-cost, speedy, and efficient system for resolving complaints. Legal processes involving lawyers and the courts to resolve interpretation issues do not fit well with this approach.

10.167 At the moment, the Privacy Commissioner cannot determine complaints under the Act and impose sanctions. That is left to the Human Rights Review Tribunal. We propose in chapter 8 that the Privacy Commissioner should have a power of determination in relation to access cases and a power to issue enforcement notices. This means that the Commissioner would become an enforcement agent under the Privacy Act. Conferring power on the Privacy Commissioner to make advance rulings on compliance with the privacy principles would not seem out of line with these proposals.

10.168 As pointed out by the Privacy Commissioner in the discussion paper cited earlier, a binding ruling power would also have significant resource implications for the Privacy Commissioner's office. It would involve costs, too, for agencies applying for a ruling. However, the Privacy Commissioner and public sector agencies currently devote considerable resources (both policy and legal) in working through the privacy implications of proposed data sharing initiatives and programmes, without necessarily achieving certainty as a result. Sometimes a legislative solution is adopted to resolve an uncertainty, but this process is also resource-intensive and often lengthy. So the costs that would be involved in a binding ruling process have to be weighed against the costs incurred as a result of the current system.

10.169 An additional issue is whether or not a binding ruling power would have an adverse effect on the Privacy Commissioner's independent role in determining complaints, as suggested by the previous Privacy Commissioner. We do not think that this is a major concern, but are keen to receive feedback on it. As we see it, the effect of a binding ruling that the Privacy Act permits certain conduct is similar to the effect of a section 54 exemption. A complaint that the activity breaches the

850 The Securities Commission discussion paper also makes this point. See Securities Commission *Binding Rulings on Securities Law: A Discussion Paper* (Wellington, June 2000).

Act is ruled out. In addition, in both cases, the beneficiary of the ruling or exemption has to stay within its terms to retain its protection. A complaint could still lie if the terms of the ruling or exemption were not adhered to.

How would a binding ruling power work?

10.170 A binding ruling power would supplement, rather than replace, the existing ways in which the Privacy Commissioner provides advice on, and attempts to clarify the application of, the Privacy Act. These include the issuing of guidelines, policy statements, case notes, explanatory material on the Commissioner's website, workshops, fact sheets, and the 0800 telephone enquiry facility. It is not envisaged that binding rulings provisions in the Privacy Act would need to be as complex as the Tax Administration Act model.

10.171 At a very general level, a binding ruling power would work as follows:

- The Privacy Commissioner would be empowered to make a binding ruling on the application of the privacy principles to a particular set of facts.
- The ruling would be binding on the Privacy Commissioner and the applicant. As long as what the applicant subsequently did was covered by the ruling, the Commissioner could not later uphold a complaint that the applicant's actions breached the privacy principles. In effect, a ruling would constitute a "safe harbour" for the applicant.
- A ruling could stipulate conditions that the applicant would need to comply with in order for the ruling to apply. Failure to comply with the conditions would take the applicant outside the protection of the ruling.

10.172 The binding ruling procedure would not be intended for day-to-day privacy issues. It should be reserved for substantial programmes or initiatives where the risk of committing time and resources could not be justified without a clear ruling on compliance with the Privacy Act. Applicants would have to show that they had fully considered the compliance issue and obtained legal advice on it, and that there was a real doubt about compliance with the Act. Requiring applicants to meet the costs of the binding ruling process might also discourage unnecessary or frivolous applications, but should not be so onerous as to act as a disincentive to agencies to make use of the process in appropriate cases.

10.173 Binding rulings would normally be made publicly available by the Privacy Commissioner, so that they could provide guidance to other agencies on interpretation of the Act. This would also alert potential complainants that the activities covered by the ruling could not be the subject of a complaint. There might be a case for keeping some rulings confidential if publicity would seriously prejudice the purpose of the activity covered by the ruling.

10.174 Rulings could cover difficult interpretation or application issues, where there is uncertainty about which side of the line the proposed initiative or programme falls on. It might also be appropriate to consider an express provision in the Act permitting the Privacy Commissioner to confirm compliance in a case of doubt, if the Commissioner is satisfied that there are no privacy-adverse consequences or that the privacy risks will be appropriately managed. Making this matter clear

in the Act might overcome problems if the Privacy Commissioner were otherwise to take the view that a binding ruling could be given only where compliance with the Privacy Act was absolutely clear.

A framework for developing proposals for specific legislative authority for data sharing

10.175 Section 13(1)(f) of the Privacy Act makes it a specific function of the Privacy Commissioner to examine any proposed legislation that makes provision for the collection of personal information by any public sector agency, or the disclosure of personal information by one public sector agency to any other public sector agency, and to report the results of that examination to the responsible Minister. Where the Privacy Commissioner considers that the information may be used for the purposes of an information matching programme, the Commissioner is to have particular regard, in the course of that examination, to the information matching guidelines set out in section 98.

10.176 So section 13(1)(f) covers general data sharing proposals, as well as specific information matching proposals. However, only in the case of information matching proposals is the Commissioner required to have regard to a set of statutorily prescribed matters.

10.177 As indicated above, specific statutory authority for data sharing by public sector agencies already exists in a number of enactments. There are advantages and disadvantages in enacting specific legislative authority to share information. On the one hand, it means that agencies are relieved from the task of applying the general provisions of the Privacy Act to a specific case. On the other hand, the existence of a specific authority in one context may cast doubt on the lawfulness of data sharing in situations not covered by the authority. Confusion, rather than certainty, may be the ultimate outcome.[851]

10.178 There may be a good case for specific legislative authority for data sharing in particular cases. However, there is currently no framework for assessing proposals for such authorities. We are told that the Ministry of Justice currently spends a lot of time working with particular agencies on some proposals. However, the lack of a proper framework runs the risk that proposals are ad hoc and context-specific, not properly thought through by the sponsoring agency, or subject to inadequate scrutiny at the policy-development stage, and that consultation with other agencies is inadequate. Furthermore, when the proposal is before Parliament for consideration, there is no set of guidelines like those applying to information matching proposals that members of Parliament can use to assess the proposal.

10.179 Consideration might therefore be given to the development and enactment of a set of data sharing guidelines similar to the information matching guidelines set out in section 98. These guidelines would serve to provide guidance to agencies in developing their legislative proposal for data sharing, and to the Privacy Commissioner and members of Parliament in assessing the proposal. The *Data Sharing Review Report* provides a good starting point:[852]

851 See Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) para 5.29.

852 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) 13.

> For anyone wishing to share personal information, the relevant questions are: What information do you wish to share? What is your purpose in sharing this information? Can you achieve your purpose without sharing the information? Are you confident that you are sharing no more and no less information than is necessary? Do you have the legal power to share the information? Do you have the technical competence to share information safely and securely? What safeguards will counter the risks that will necessarily arise as a result of sharing? By what means and on what basis did you or will you acquire the information? The answers to these questions provide the basis for designing and evaluating any proposal to share information.

10.180 Further, in chapter 9, we noted that the ability of the Privacy Commissioner to properly assess a proposed information matching programme in accordance with section 98 depends in large part on the information provided to the Commissioner by the relevant agencies sponsoring the proposal. We suggested that a statutory requirement on the sponsoring agencies to supply the Commissioner with a "programme protocol" would highlight the need for agencies to undertake the necessary policy spadework when developing an information matching proposal, and facilitate assessment of the proposal by the Commissioner.

10.181 The same is true with respect to data sharing proposals, and we make the same suggestion in this context.

Providing greater transparency and accountability for data sharing in the public sector

10.182 We noted in chapter 9 that the Privacy Act has specifically dealt with information matching by government agencies from the outset because of the particular privacy issues that it raises. We suggested there that, given that data mining raises similar issues, and the enormous scope for its use (and misuse) in relation to the vast amount of personal information now available online, it may now be time to consider greater controls. One possible starting point might be to require greater transparency and openness about data mining in New Zealand, and to impose a requirement on public agencies to report on their data mining activities.

10.183 Data sharing raises much the same issues. Both issues highlight the importance of public trust in government. If citizens are suspicious about what information about them is shared, then they may cease cooperating and providing information. Greater openness and reporting might help to allay citizens' suspicions about what government agencies are doing with their personal information, and maintain or enhance trust and confidence in government.

10.184 The Thomas/Walport report makes this point very strongly: "Improving transparency about the extent and nature of sharing of personal information is an important measure that could improve knowledge and trust, allay suspicions

about the nature of data sharing and stimulate public debate."[853] Transparency, understanding, and trust with respect to government use of personal information might then flow through into improved public services:[854]

> Only when people better understand what happens to their personal information will they invest more trust in the organisations that process it. And only when levels of trust are suitably high will organisations be able to take full advantage of the potential benefits offered by the use of personal information, passing on those benefits to the public through more efficient, better-value services.

10.185 The information matching provisions of the Privacy Act require agencies involved in authorised information matching programmes to make such reports to the Privacy Commissioner in respect of the programmes as the Commissioner from time to time requires.[855] The Commissioner must report on active authorised information matching programmes in her annual report.[856]

10.186 A first step towards greater transparency with respect to information sharing might be to require public sector agencies that rely on specific legislative authority for information sharing as part of their activities to report annually on their usage of that authority. This requirement might be similar to the requirements relating to reporting on information matching, except that each agency would report separately rather than provide material for publication by the Privacy Commissioner.

10.187 Where specific legislative provision is made for information sharing agreements, such as those authorised by the Corrections Act and the Passports Act, consideration might be given to requiring these to be publicly available (unless to do so would be likely to frustrate the objective of the agreement).

10.188 In the preceding paragraphs we have been concerned only with information sharing authorised by specific statutory provisions. A broader reporting regime with respect to information sharing by public sector agencies might be considered once the practical operation and value of a narrower regime is able to be assessed. On the other hand, it might be thought that such detailed reporting is "overkill", and that it might be enough for agencies simply to report on the *fact* of an information-sharing arrangement. The Privacy Commissioner might then report an annual list of "live" sharing arrangements.

---

853 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) paras 6.6–6.7.

854 Richard Thomas & Mark Walport *Data Sharing Review Report* (London, 2008) para 8.13. See also the comments by the UK Advisory Panel on Public Sector Information, in its 2008–09 Annual Report (July 2009). The comments are made in the context of the re-use of public sector information, but nevertheless resonate as well in the context of government information sharing. The Panel said (at page 20):

> We are convinced that widespread re-use of PSI will only be achieved if members of the public are confident that personal information is protected; that there are robust and transparent processes to control and monitor the sharing of information; and that public and private sector bodies are held accountable for any unauthorised or inadvertent sharing of personal data. To realise the value of PSI, we need to inspire confidence and this means a radical shift in personal and organisational cultures. Thus knowledge and information management will be the lynchpin of transformational government as well as beneficial to PSI re-use.

855 Privacy Act 1993, s 104.

856 Privacy Act 1993, s 105.

An exception to principle 11

10.189 Principle 11 prohibits disclosure of personal information unless the disclosure falls within one of nine exceptions. The first of them is capable of allowing the sharing of information in a significant number of cases:

> that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained.

It may be that the enabling potential of this provision is not fully realised by some agencies.

10.190 Another exception enables sharing in a more limited range of circumstances:

> (f) that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to–
>
> (i) public health or public safety; or
>
> (ii) the life or health of the individual concerned or another individual.

We have already suggested, in chapter 4, that this provision might be enhanced by the removal of the "imminence" requirement. It may also be worth considering whether paragraph (f)(ii) might be broadened, or a new exception added, to cover the case where the information is disclosed to prevent or lessen a threat to the *welfare* of the individual. Such a provision appears in the Information Privacy Act 2000 of Victoria, which includes an exception for disclosure that was reasonably believed to be necessary to lessen or prevent "a serious and imminent threat to an individual's life, health, safety or *welfare*".[857]

10.191 A similar exception is proposed in the Information Privacy Bill 2007 of Western Australia, although there the word "imminent" does not appear. Given that the term "welfare" is capable of wide interpretation, careful consideration would be needed before adopting such a proposal, and, if adopted, in framing the exception. We would welcome views on it.

Extend section 54 exemption power

10.192 Section 54 of the Privacy Act empowers the Privacy Commissioner to exempt certain activities from compliance with certain privacy principles.[858] The Commissioner can authorise an agency to collect, use, or disclose personal information, even though this would otherwise breach principles 2, 10 or 11, if the Commissioner is satisfied, in the special circumstances of the case, that the public interest outweighs any interference with the privacy of the individual that could result, or that there is a clear benefit to the individual concerned that outweighs any such interference.

857 Information Privacy Act 2000 (Vic) Schedule 1, Principle 2.1(d)(i).

858 For a detailed discussion of section 54, see chapter 5.

10.193 While authority to share data could be sought by public sector agencies under section 54, the provision is of limited usefulness in this context. As currently applied by the Privacy Commissioner, section 54 permits the granting of one-off exemptions, rather than generic or ongoing exemptions.

10.194 The Australian Federal Privacy Act, and privacy legislation in some Australian states and territories, confer wider exemption powers than provided by section 54. These powers are outlined in paragraphs 10.98 and 10.107–10.113 above.

10.195 Section 54 of the NZ Privacy Act could be extended along the lines of the Australian PID model so as to empower the Privacy Commissioner to authorise data sharing initiatives or programmes proposed by public sector agencies in appropriate cases. Specific components of the extended exemption power might include the following:

- The power might be restricted to the granting of exemptions for public sector agencies only, or might be restricted even further, so that it applies only with respect to data sharing initiatives or programmes (either generally or of a specific kind).
- Applicants for an exemption might be required to submit a privacy impact assessment relating to the proposed data sharing initiative.
- The Australian Federal Act threshold (the public interest outweighs, to a substantial degree, the public interest in adherence to the privacy principles) would seem to be appropriate, and would be consistent with the current formulation of the threshold test in section 54.
- Consultation and publication requirements, which are not currently part of the section 54 procedure, should be included, along the lines of those currently required with respect to the issuing of codes of practice under section 46.
- A requirement might be imposed on agencies invoking the exemption to report on the activities carried out under it.
- Exemptions might be treated as regulations for the purposes of the Regulations (Disallowance) Act 1989, so as to provide for Parliamentary supervision and control over the use of the power.

10.196 With respect to the guiding principles we identified above, this option permits the propriety of particular data sharing initiatives to be judged by the Privacy Commissioner on a case-by-case basis; uses a proportionality test to determine whether or not the granting of an exemption is appropriate; allows the risk of the proposed sharing to be assessed, and mitigations to be put in place through the imposition of conditions on an exemption; and imposes transparency and accountability requirements. For public sector agencies, the option would be reasonably flexible (depending on how wide the exemption power was cast), but not particularly speedy.

10.197 However, this option takes a reasonably broad brush approach to the issue, and potentially creates a large hole in the protections currently provided by the Privacy Act when the problem sought to be addressed is possibly small in scope and scale.

A schedule of authorised data sharing initiatives

10.198 Part 11 and Schedule 5 of the Privacy Act set up a special and very simple regime with respect to the disclosure of law enforcement information that overrides the privacy principles. Particular information about an individual is specified in Schedule 5 as being held by a public sector agency (the holder agency), and other public sector agencies (accessing agencies) may have access to that information if Schedule 5 authorises it. We examine this mechanism in detail in chapter 12. Schedule 5 could originally be amended by Order in Council, but this power has expired.

10.199 This mechanism could be adopted to authorise particular data sharing between public sector agencies outside the law enforcement context. Schedule 5 was originally populated with existing (and reasonably stable) law enforcement information sharing arrangements under the Wanganui Computer Centre Act 1976. A new data sharing schedule would need to be created from scratch, so as to identify particular public sector agencies and the personal information they hold, and identify other public sector agencies with which that information could be shared and the purposes for which the information could be shared. It would be possible to specify in the schedule particular conditions on the authority to share data, or provide for these to be imposed by the Privacy Commissioner.

10.200 Given the wide variety of data sharing arrangements that might need to be included in the schedule, a power to amend the schedule by Order in Council would seem necessary so that new data sharing initiatives could be authorised as the need arises. A prerequisite to the making of an order might be consultation with the Privacy Commissioner, or even a recommendation from the Privacy Commissioner. A proportionality test could be built into the Order in Council mechanism, by requiring the Minister recommending the making of the order, or the Privacy Commissioner, to be satisfied that the public interest in authorising the data sharing outweighs adherence to the privacy principles.

10.201 Agencies proposing the addition of new initiatives for authorisation in the schedule might be required to undertake a privacy impact assessment as part of the process of assessment for each proposal, and there might also be a requirement on agencies to report publicly on activities undertaken in reliance on the authority.

10.202 With respect to the guiding principles outlined earlier in the chapter, this option permits the propriety of particular data sharing initiatives to be judged on a case-by-case basis; could include a proportionality test to determine whether or not the granting of an exemption is appropriate; could allow the risk of the proposed sharing to be assessed, and mitigations to be put in place through the imposition of conditions on an authority; and imposes transparency and accountability requirements. For public sector agencies, the option would be reasonably flexible, but (as with the exemption power option) not particularly speedy.

10.203 A possible unintended consequence of a schedule 5 approach would be for agencies to regard the schedule as the sole authority for data-sharing activities. The schedule might then, rather perversely, operate as a constraint on data sharing, regardless of the more general application of the privacy principles.

This has already been identified as a problem with the existing Schedule 5. The process might also be seen as unnecessarily bureaucratic, and suitable only for major initiatives.

A new regime similar to the existing information matching regime

10.204 This option can be outlined very briefly. It would mirror the current provisions of the Act relating to information matching. There would be a new Part in the Privacy Act relating to data sharing, containing standard provisions and a set of data sharing rules similar to the information matching rules. Information sharing would require a specific statutory authority to be enacted in each case, which would be included in the appropriate enactment and referenced in a new schedule to the Privacy Act (as with existing schedule 3). Standard reporting and accountability provisions would apply.

10.205 This option would also incorporate the options mentioned above, for the enactment of an equivalent of section 98 containing information sharing guidelines, and for a statutorily mandated framework for assessing information sharing proposals.

10.206 With respect to the guiding principles identified above, this option permits the propriety of particular information sharing initiatives to be judged on a case-by-case basis; could use a proportionality test to determine whether or not the granting of an authority is appropriate; could allow the risk of the proposed sharing to be assessed, and mitigations to be put in place through the imposition of conditions on an authority; and imposes transparency and accountability requirements.

10.207 For public sector agencies, the option would be reasonably flexible in terms of scope. However, being integrated into the legislative process, it would not ordinarily provide a timely way of gaining authority for data-sharing initiatives, and might not provide for the wide range of initiatives which might prove desirable.

A "common or integrated programme or service" exception (Alberta/British Columbia model)

10.208 This option would involve amending principle 11 by adding a new ground for the disclosure of personal information along the lines of the "common or integrated programme" exception in the Alberta and British Columbia privacy legislation. The legislation permits public bodies to disclose personal information to another public body if the disclosure is necessary for the delivery of a common or integrated programme, activity or service, and for the duties of the person to whom the information is disclosed.

10.209 As interpreted in Canada, a common programme or service is a single programme or service that is provided or delivered by two or more agencies. An integrated programme or service is a programme or service that has several distinct components, where each component may be provided or delivered by a separate agency, but together the components make up the programme or service.

10.210 This option would potentially create a very broad information sharing power for public sector agencies. Unlike the earlier options, where agencies would have to apply for an exemption from the ordinary provisions of the Privacy Act and substantiate the case for it, this option would not require the agencies, type of personal information, or purpose of the information sharing to be authorised in advance. Nor would the option impose any transparency and accountability requirements on agencies invoking the exception.

10.211 The Canadian legislation does not specify any particular procedural requirements that must be complied with before the exception can be invoked. Detailed guidance material has been issued by the Alberta Ministry of Service, including suggested criteria for determining the applicability of the exception, and advice on undertaking a privacy impact assessment, consultation with the Information and Privacy Commissioner, the use of information sharing agreements between the agencies involved, and the provision of information to individuals whose personal information is involved. The British Columbia provision has been interpreted very strictly by the British Columbia Information and Privacy Commissioner, and it has therefore been very difficult for agencies to use it.

10.212 It would be possible for any New Zealand version of the exception to be supplemented by guidelines issued by the Privacy Commissioner, or Cabinet-mandated procedural requirements.

10.213 A variation to the Canadian model could also permit data sharing with NGOs, where their involvement in the common or integrated programme or activity required it.

10.214 With respect to our principles, this option permits the propriety of particular information sharing initiatives to be judged on a case-by-case basis; does not explicitly involve a proportionality test to determine whether or not the overriding of the privacy principles is appropriate; does not explicitly require the risk of the proposed sharing to be assessed, or mitigations to be put in place through the imposition of conditions; and does not impose any express transparency or accountability obligations.

10.215 For public sector agencies, this option would potentially be reasonably easy to use, being very flexible in terms of scope, although procedural preconditions might limit this flexibility. However, as an exception to principle 11, the applicability of the new provision in any particular case would be determined after the fact by the Privacy Commissioner and the Human Rights Review Tribunal in the context of a complaint. Unlike some other options identified above, public sector agencies would therefore have no assurance of compliance in advance.

10.216 If it were felt that such a broad exemption from principle 11 is not justified, consideration might be given to exempting a "common or integrated" programme for defined, limited purposes: for example, to allow the sharing of health information.

A variation of the "common or integrated programme" solution

10.217 A variation of the "common or integrated programme" solution, although with more formal controls, has been canvassed in earlier work by the Ministry of Justice. This option would amend the Privacy Act to allow public sector agencies to share personal information for common or integrated programmes, where those programmes deliver services to common clients. Principles 2, 10 and 11 would be overridden. The mechanism would cover government departments, Crown entities, Crown agencies, and NGOs contracted to provide public functions. To qualify as a "common or integrated programme", a programme would require multi-agency cooperation to deliver a service, where the service is for a "beneficial social outcome". This would cover the delivery of a service or services to an individual or a group of individuals; for example, a young offender, family, or a group of people living in a particular neighbourhood or location. The mechanism would extend to the sharing of information in order to identify people who are common clients of the participating agencies and to deliver services to such people. Personal information could not be shared for the purpose of taking adverse action against an individual.

10.218 Prior government approval for agencies to take advantage of the new mechanism for an individual programme would be required. This approval would take the form of inclusion of the programme (but not individual initiatives within the programme) in a schedule to the Privacy Act by Order in Council. The approval would list the name of the programme, its purposes, the participating agencies, and the nature of the personal information to be shared under the programme.

10.219 Participating agencies wishing to invoke the mechanism for a particular programme would need to show that they had considered whether other information sharing mechanisms available under the Act (such as exceptions to principle 11, or information matching) could be used, and would be required to consult with the Privacy Commissioner on the development of the programme. Agencies would be required to publish information about the programme and report annually on its operation, and the Privacy Commissioner could request the participating agencies to review the operation of the information sharing under the programme. An additional safeguard would be to permit individuals to opt into the programme, or opt out of the programme.

10.220 With respect to the guiding principles outlined above, this option permits the propriety of particular information sharing initiatives to be judged on a case-by-case basis; does not explicitly involve a proportionality test to determine whether or not the overriding of the privacy principles is appropriate; could allow the risk of the proposed sharing to be assessed, and mitigations to be put in place through the process for developing a proposal for approval by Order in Council; and would impose transparency and accountability obligations. A possible difficulty with this mechanism is the vagueness of some of the concepts, such as whether or not a service to be delivered by an approved programme is for a "beneficial social outcome".

10.221 For public sector agencies, this option, while reasonably wide in scope, would impose significant procedural requirements that might limit its flexibility. However, the Order in Council mechanism for approving programmes to which the mechanism applied would provide agencies with the certainty that flows from prior approval of the programme.

Other options

10.222 A number of variations or combinations of the previous options are possible. To identify all of these is not practicable, and we have not attempted to do so. Other options that we do not explore here include:

- Undertaking a review of other legislation that may inhibit information sharing, and amending it where necessary. This would be a similar exercise to that undertaken by the Information Authority under the Official Information Act 1982. The Authority was required by that Act, among other things, to review the protection accorded to official information by any Act with a view to seeing whether that protection was reasonable and compatible with the purposes of the Act.[859] A review with respect to the Privacy Act might be undertaken by the Privacy Commissioner or the Law Commission.
- Permitting the exchange of personal information by public authorities for specified purposes, regardless of any statutory confidentiality or secrecy provisions. This is the approach in Part 6 of the Western Australian Information Privacy Bill.[860] This would reverse the current approach in the Privacy Act, which generally gives way to other legislation.
- Imposing a statutory duty on public bodies to share information except in defined circumstances, as recommended in Ireland.[861]

10.223 As well as comments on the options that we have put forward, we would welcome any other suggestions about how the sharing of information by public sector agencies might be facilitated in appropriate cases.

859 Official Information Act 1982, s 38(1)(a) (expired).

860 See paragraphs 10.112–10.113 above.

861 See paragraph 10.115 above.

Q122 We have presented the following mechanisms as possible means of regulating information sharing:

- guidelines;
- a code of practice;
- a national public sector information sharing strategy;
- a rebuttable presumption that personal information held by one public sector agency can be shared with other public sector agencies if such sharing is for the benefit of the individual concerned and is for a purpose that is broadly similar to that for which the information was obtained;
- allowing the Privacy Commissioner to issue binding or advance rulings;
- the enactment of a set of information sharing guidelines similar to the information matching guidelines in section 98;
- requiring greater openness about information sharing by public sector agencies (such as requiring them to report annually on their information sharing activities);
- the addition of a new "welfare" exception to principle 11;
- an extension of the current section 54 exemption power;
- a schedule of authorised information sharing activities;
- a new regime similar to the existing information matching regime; and
- a "common or integrated programme or service" exception.

What are your views on any of these mechanisms?

Q123 Do you have any other suggestions about how the sharing of information by public sector agencies might be facilitated in appropriate cases?

CROSS-BORDER INFORMATION SHARING

10.224 This chapter is concerned mainly with sharing of personal information between government agencies within New Zealand. However, we are aware that sharing of personal information between government agencies in New Zealand and those in other jurisdictions is assuming increasing importance. In particular, there is a growing interest in the sharing of information between Australia and New Zealand, especially in relation to law enforcement matters.[862] There is a question about how best to provide legally for such information sharing, including how to ensure that privacy of information is protected.

10.225 Options for providing legal authority for cross-border sharing of personal information between government agencies might include:

- inserting a framework for such cross-border sharing into the Privacy Act; or
- making legislative provision in other primary legislation for entering into information-sharing arrangements with other countries.[863]

Each of these options would need to provide for safeguards, including some form of oversight by the Privacy Commissioner. There may also be other options.

10.226 We invite submissions on these options, or suggestions for other ways in which this issue could be handled. The Ministry of Justice is working on this issue, and the Law Commission will pass on submissions dealing with cross-border information sharing to the Ministry to assist them with their work.

Q124 How should legal authority for sharing of personal information across borders between government agencies be provided for? How should the law ensure that privacy is protected when information is shared in this way?

862 See chapter 12 for discussion of this issue in the law enforcement context.

863 See, for example, Customs and Excise Act 1996, ss 281, 282, 282A(4); Immigration Act 2009, ss 305–306. See also the provisions of the Social Welfare (Transitional Provisions) Act 1990, ss 19-19D, discussed in chapter 9. There are guidelines for legislative provisions authorising the transfer of personal information outside New Zealand in Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (2001 edition, most recently amended 2007) 322–323.

Chapter 11

Interaction with other laws

11.1 This chapter considers issues about the Privacy Act's interaction with other statutes and laws. First we look at matters of statutory interpretation, such as the suitability of the Privacy Act's section 7 as a deferral mechanism to other law, whether section 7 should be redrafted, and whether additional aids to statutory interpretation are needed, such as a comprehensive list of legal provisions that override the privacy principles. Then we examine two generic statutory schemes that interact with the Privacy Act, namely the official information legislation (the Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987) and the Public Records Act 2005. Other important statutory frameworks that interact with the Privacy Act are the Health Act 1956 and the Health and Disability Commissioner Act 1994. The Health Act is discussed in chapter 19. We briefly consider in this chapter the interrelationship between the Privacy Act and the Health and Disability Commissioner Act. We also briefly consider the Statistics Act 1975, and statutory secrecy provisions.

THE SUBSERVIENCE OF THE PRIVACY PRINCIPLES TO OTHER LEGISLATION

11.2 The privacy principles set out a default position for the handling of personal information; however, other legislation may expressly or impliedly override the principles, either by imposing stricter requirements than those imposed by the principles,[864] or authorising disclosure or practices that may otherwise breach the privacy principles. The subservience of the privacy principles to other statutory provisions is due to the operation of principles of statutory interpretation such as *generalia specialibus non derogant* (general provisions do not derogate from specific ones).[865] In addition, section 7 of the Privacy Act is a ranking provision, confirming that the principles may be overridden by other laws, and making clear that the privacy principles are subservient to legislative provisions in force at the time that the Privacy Act was passed, as well as those that have been subsequently enacted.[866] The principles therefore provide a general framework for the handling of personal information, although with the flexibility that the principles or particular aspects of them may be modified or overridden

864 For example, statutory obligations of secrecy or non-disclosure.

865 See JF Burrows and RI Carter *Statute Law in New Zealand* (4th ed, LexisNexis, Wellington, 2009) 457–461.

866 See generally JF Burrows and RI Carter *Statute Law in New Zealand* (4th ed, LexisNexis, Wellington, 2009) 470–471.

in certain contexts by other legislation. This means that the privacy principles cannot be read on their own, as reference must be had to other relevant legislation that may modify or change the operation of the principles in certain contexts.

PRIVACY COMMISSIONER'S CONSULTATION WITH OTHER BODIES AND REFERRAL OF COMPLAINTS

11.3 As well as the general function to consult with other bodies concerned with privacy,[867] the Privacy Commissioner may consult in particular with the Ombudsmen,[868] the Health and Disability Commissioner[869] and the Inspector-General of Intelligence and Security[870] in relation to any matter arising out of a Privacy Commissioner investigation under Part 8 of the Privacy Act, or any other matter relating to the Privacy Commissioner's functions that is within the jurisdiction of the other body, or for the purposes of determining under which legislation a privacy complaint should be dealt with. The Ombudsmen Act 1975 provides a reciprocal consultation provision under which the Ombudsmen may consult with the Privacy Commissioner in relation to any matter relating to the Ombudsmen's functions.[871] The Ombudsmen also have a duty to consult the Privacy Commissioner when investigating complaints about the withholding of official information on privacy grounds.[872] A protocol has been drafted to reflect the consultation process between the Privacy Commissioner and the Ombudsmen.[873]

11.4 These provisions encourage dialogue between the various agencies responsible for different aspects of information handling by agencies. In an earlier review, the Privacy Commissioner noted that while the provisions are necessary to overcome the duty of secrecy otherwise imposed on the Privacy Commissioner that otherwise applies, they were also intended to foster co-operation between the various agencies and to avoid duplication of process.[874]

11.5 As well as consultation, the Privacy Act also provides for the Privacy Commissioner to refer privacy complaints or particular aspects of privacy complaints to these other bodies, if the Commissioner considers that the matter would fall more appropriately within their jurisdiction.[875] These referral provisions provide the necessary flexibility for the Privacy Commissioner to transfer privacy complaints or aspects of them to the most appropriate body.

867 Privacy Act, 1993, s 13(1)(j). See further chapter 4.

868 Privacy Act 1993, s 117. See Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) INT.4 (last updated 2007).

869 Privacy Act 1993, s 117A.

870 Privacy Act 1993, s 117B.

871 Ombudsmen Act 1975, s 29B.

872 Official Information Act 1982, s 29B. See also the Local Government Official Information and Meetings Act 1987, s 29A.

873 This protocol is currently in draft form.

874 *Necessary and Desirable* para 12.4.1.

875 Privacy Act 1993, ss 72, 72A and 72B.

STATUTORY INTERPRETATION

Deferral to other law under section 7

11.6 Section 7(1) to (3) deals specifically with privacy principles 6 (access to a person's own personal information) and 11 (disclosure):

- Principles 6 and 11 do not derogate from any provision in any *enactment* (that is, an Act or regulation) that authorises or requires personal information to be made available.
- Principles 6 and 11 do not derogate from any provision in an *Act of Parliament* that imposes a prohibition or restriction in relation to the availability of personal information (that is, statutory secrecy provisions) or regulates the manner in which personal information may be obtained or made available.
- Principles 6 and 11 do not derogate from any provision in existing *regulations*[876] that imposes a prohibition or restriction in relation to the availability of personal information or regulates the manner in which personal information may be obtained or made available.

11.7 Section 7(4) deals with the privacy principles other than principles 6 and 11, confirming that these principles defer to other legal provisions. The effect of section 7(4) is to defer these privacy principles to both the common law and statute law, including delegated legislation such as regulations.[877]

11.8 Section 7(5) expressly disapplies principle 7 (correction of personal information) in relation to information obtained and held by the Department of Statistics under the Statistics Act 1975.

Issues with section 7

11.9 There are several issues with section 7:

- Overall, the section is complicated, opaque and not user-friendly.
- There is no easy reference point to locate legislation that overrides the privacy principles. For example, it is not clear which regulations prevail over the privacy principles and which do not.
- A more detailed approach is taken to the interaction of principle 6 (access to personal information) and principle 11 (disclosure of personal information) with other law (section 7(1), (2), (3)) than the interaction of the other principles with other law (section 7(4)). Because of the inverse relationship between principles 6 and 11, grouping them together in the provision is also a complicating factor.

876 This non-derogation is limited to regulations made by Order in Council that were in force immediately before 1 July 1993 (that is, before the Privacy Act came into force), or, in relation to public sector agencies, before 1 July 1983 (before the Official Information Act came into force), or, in relation to local authorities and related public sector agencies, before 1 March 1988 (that is, before the Local Government Official Information and Meetings Act 1987 came into force).

877 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) PVA 7.5 (last updated 2007).

- The title of the section does not add clarity. "Savings" is generally used to specify legislation that is saved from repeal. However, there is no issue of repeal in this context; the issue is one of statutory precedence.[878]

11.10 Section 7 of the Privacy Act was considered by the Privacy Commissioner in *Necessary and Desirable*.[879] That report made recommendations for simplification and clarity of the ranking provision, and raised a number of options including:[880]

- simplification of section 7 and drafting the provision in a straightforward manner whereby its effect is plain;[881]
- a new marginal note;
- reverting to formulations used in the Privacy of Information Bill[882] (the precursor to the Privacy Act) such as expressly including disclosure under the Official Information legislation as an exception to principle 11,[883] and precluding principle 11 from authorising breaches of secrecy obligations and non-disclosure requirements;[884]
- moving elements of section 7 into the relevant privacy principles or sections of the Act as exceptions to the principles;[885]
- disentangling the principle 11 issues from the principle 6 issues in section 7(2) and (3);
- phasing out section 7(3) altogether; and
- maintaining a rump of section 7 after relocating certain aspects.[886]

11.11 We think that section 7 is unduly complex, and agree with the Privacy Commissioner that it should be redrafted.

Q125 We propose that section 7 should be redrafted. Do you agree? Do you have any particular comments or suggestions for approaching this?

878 In *Necessary and Desirable* 6, the Privacy Commissioner noted that "savings" is a technical legal term that is not readily understood by lay readers of the Act. For other options see for example Private Schools Conditional Integration Act 1975, s 80 (Relationship between this Act and other enactments) and New Zealand Walkways Act 1990, s 7 (Conflict with other Acts) (since repealed).

879 *First supplement to Necessary and Desirable* 92–101.

880 *Necessary and Desirable* recommendations 30–34.

881 See for example Information Privacy Act 2000 (Vic), s 6.

882 The select committee considering the Privacy of Information Bill made the decision to bring all the savings provisions affecting the privacy principles together, which increased the level of complexity in section 7.

883 The Privacy of Information Bill, cl 8, principle 14(1)(d) contained the following exception: "The disclosure is made pursuant to any provision of the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987." Principle 14 in the Bill became principle 11 in the Privacy Act.

884 The Privacy of Information Bill, cl 8, principle 14(2) contained the following proviso to the disclosure principle: "Nothing in subclause (1) of this principle shall be taken as authorising the disclosure of any personal information in any case where the disclosure of that personal information would be a breach of any obligation of secrecy or non-disclosure imposed by the provisions of any enactment." Principle 14 in the Bill became principle 11 in the Privacy Act.

885 See Bob Stevens "The Review's Treatment of the Information Privacy Principles" [1998] PLPR 82, for a critique of the proposal to distribute elements of section 7 among the relevant privacy principles.

886 *Necessary and Desirable* paras 2.15.43–2.15.45.

List of statutory overrides

11.12 One of the issues with section 7 is that there is no readily available list of the legislative provisions that override the privacy principles. It is not known precisely how many enactments the Privacy Act is subject to in one respect or another, but there were at least several hundred at the time the Privacy Act came into force.[887]

11.13 For ease of reference and to enhance the user-friendliness of the Privacy Act, ideally references to all statutory provisions that override the privacy principles should be collected together and a list should be readily available to the public. A list of this sort would provide a legislative map of relevant legislation and act as a guide to the interpretation of the generic provisions of the Privacy Act. Because the statutory overrides are essentially further exceptions to the privacy principles, it is difficult for users of the Act to understand or apply the privacy principles without having access to this information. A collection of statutory override provisions would also assist the process of statutory review and consistency. Another potential benefit is that the Privacy Act itself could be streamlined by moving provisions relating to specific issues to particular legislation.[888]

11.14 The Australian Law Reform Commission (ALRC) considered whether a comprehensive list should be compiled of legislative provisions that require or authorise acts that would otherwise be regulated by the Australian Privacy Act, to provide clarity as to the circumstances in which the Privacy Act is overridden.[889] The ALRC concluded that this would require significant resources and recommended instead that the Australian Privacy Commissioner should publish guidance on when an Act will be required or authorised by or under law such that it will override the privacy principles, with examples.[890]

11.15 The exercise of identifying all the statutory overrides necessary to compile a comprehensive list would be far from straightforward and, as noted by the ALRC, would involve significant resources. In particular, it would be difficult to identify potential implied overrides of the principles. However, we suggest that there are a range of options for a list of overrides, some of which would be less resource intensive than others.

11.16 Possible options we have identified include:

- a new Schedule to the Privacy Act containing a comprehensive list of statutory overrides by way of cross-reference;
- a new Schedule to the Privacy Act containing a non-exhaustive table of key overrides (this could be subject to annual amendment to capture additional overrides identified);

887 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) PVA 7.6 (last updated 2007).

888 See, for example, Privacy Act 1993, s 7(5) (statistics); s 55 (certain personal information excluded); s 57 (intelligence organisations).

889 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 16.96–16.109.

890 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 16-2.

- a comprehensive list of statutory overrides compiled by the Office of the Privacy Commissioner (OPC) (or another agency) and published as guidance or educational materials; or
- a working list of statutory overrides compiled by the OPC (or another agency) which could be updated annually or from time to time as the Office identifies relevant provisions through forming a view in the context of considering complaints, through the review of new legislation and otherwise, and as matters of interpretation are dealt with by the Tribunal; agencies could also submit to the OPC for consideration for inclusion in the list, potential overrides on which they wish to rely.

11.17 A list in the form of a Schedule to the Privacy Act would carry greater weight than a list produced in the form of guidance. A list in statutory form could clarify any areas of uncertainty or inconsistency, but a Schedule may be less flexible as it would need to be amended as new statutory overrides are created. It would also create an impression that it was exhaustive, whereas it might be difficult to ensure that that was in fact the case, as will be demonstrated in the next section. However, the process of statutory amendment would promote more thorough analysis of the interaction between the Privacy Act and other statutory provisions.

11.18 A non-exhaustive list could capture key overrides relatively easily, without requiring the resources necessary to compile a comprehensive list. The agency tasked with producing the list of overrides could consult with other agencies, or hold a forum to gather together the relevant provisions that are commonly relied on as overrides to the principles.

Q126 Do you think a published list or table of statutory provisions that override the privacy principles would be helpful? In what form should this be made available?

Statutory override of the privacy principles

11.19 The interaction of other legislation with the privacy principles produces significant complexity. The principles are subject to both express and implied amendment by other statutes and regulations. Overrides may be in the nature of blanket overrides, or may only arise in certain circumstances.[891] Overrides may oust one or more of the privacy principles, while leaving other privacy principles unaffected. We think that there are two issues that warrant further consideration:

- the scope for implicit override of the privacy principles by other legislation; and
- the scope for the privacy principles to be overridden by delegated legislation.

891 See discussion of the relationship between the Tax Administration Act and principle 6: Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) PVA7.8 (last updated 2007).

Implied statutory overrides

11.20 The particular difficulty with implied statutory overrides is that there may be nothing on the face of a statutory provision to suggest that an override of certain privacy principles is a necessary consequence. An implied override was identified by the Human Rights Review Tribunal in *Clearwater v Accident Compensation Corporation*.[892] The Tribunal found that while a provision in the Accident Insurance Act that an insured person's employer was entitled to be present at a review hearing did not expressly authorise disclosure to an employer of materials relevant to the review, it found the employer's right to receive the relevant information to be implicit due to the operation of section 7(1) of the Privacy Act.

11.21 The scope for implicit override provides a degree of flexibility in reconciling the privacy principles with other legislation. Without this flexibility, competing legislation would need to be clearly expressed to override the privacy principles, and legislation which failed to be sufficiently express may be ineffective. On the other hand, it may be difficult to identify an implied override, both for agencies utilising the principles and for complainants, and indeed an override may not be established until tested by a complaint or proceedings. There is also the possibility that implied amendment of the privacy principles is an unforeseen and unintended consequence of subsequent legislation.

11.22 One option would be adopting in the Privacy Act the presumption used in the Bill of Rights Act that in the case of real ambiguity, a meaning consistent with the Privacy Act is to be preferred where that is possible.[893] This would strengthen the privacy principles against implicit overrides, at least where there is ambiguity as to whether other legislation produces an override or not.

11.23 Another option would be to provide a mechanism for agencies to request an opinion or view from the Privacy Commissioner as to whether a statutory provision constitutes an override of the privacy principle. This would provide agencies seeking to rely on an override with a greater degree of certainty as to the interrelationship of legislation with the privacy principles, outside the context of a specific complaint. The Privacy Commissioner could also pronounce a view on a particular override on her own motion, if she became aware of an industry practice of reliance on a statutory override. The Privacy Commissioner does not currently have the power to make rulings, although we raise this as an option in chapter 10. We note that this option is somewhat problematic as there is always the possibility that the Tribunal or a court may not agree with the Privacy Commissioner's interpretation. If the ruling was non-binding, an agency relying on the ruling may therefore be exposed to unexpected liability. If the ruling was binding, a complainant would be unable to challenge any breach of the principles by an agency relying on the ruling. We outline the issues associated with binding rulings in chapter 10. One of the Commissioner's current functions is to provide advice (with or without a request) to an agency on any matter

892 (23 February 2004) HRRT Decision No 02/04, noted in Office of the Privacy Commissioner *Human Rights Review Tribunal Privacy Cases January 2003 – February 2005* (Wellington, 2005) 283. Also discussed in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) PVA 7.7 (last updated 2007).

893 New Zealand Bill of Rights Act 1990, s 6.

relevant to the operation of the Privacy Act.[894] This would allow agencies to seek the Commissioner's view of an override; however, any such advice is non-binding and it would be open for the Commissioner to take a different view in the event of a complaint, and for the Tribunal to take a different view. The Privacy Commissioner's advice to an agency is not made publicly available to inform others about the Commissioner's interpretation, although the Privacy Commissioner could make her view public.

11.24 We have also considered whether there should be a specific requirement for the Privacy Commissioner to report to Parliament on any Bill that appears to be inconsistent with the privacy principles. This could build on some of the Privacy Commissioner's current functions, such as the function to examine any proposed legislation that makes provision for the collection or disclosure of personal information by public sector agencies,[895] and the function to examine any proposed legislation or proposed government policy that may affect the privacy of individuals,[896] in each case reporting to the responsible Minister. However, we note that the Legislation Advisory Committee guidelines for legislation[897] and the Cabinet Office Manual both contain guidance on the need for new legislation to be consistent with the privacy principles. The Cabinet Office Manual requires Ministers to certify that proposed legislation complies with the privacy principles and permits the Privacy Commissioner to express an independent view in the Cabinet paper. In light of these measures, a further reporting function for the Privacy Commissioner would not seem to be necessary.

Override by delegated legislation

11.25 The second issue we raise in this section is the potential for the privacy principles to be overridden by delegated legislation. Currently, section 7 is confusing and unsatisfactory on this issue.

11.26 Section 7(1) provides:

> Nothing in principle 6 or principle 11 derogates from any provision that is contained in any enactment and that authorises or requires personal information to be made available.

"Enactment" is defined as any Act of Parliament or any regulation within the meaning of the Regulations (Disallowance) Act 1989.[898]

894 Privacy Act 1993, s 13(1)(l).

895 Privacy Act 1993, s 13(1)(f).

896 Privacy Act 1993, s 13(1)(o).

897 Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2007) chapter 15.

898 Privacy Act 1993, s 2.

11.27 Section 7(3) is a complex provision which (in summary) provides that nothing in principles 6 or 11 derogates from any provision in a regulation (within the meaning for the Regulations (Disallowance) Act 1989) which was in force (at various times) before the Privacy Act 1993, and which:

(i) imposes a prohibition or restriction in relation to the availability of personal information; or

(ii) regulates the manner in which personal information may be obtained or made available.

11.28 Section 7(4) provides:

> An action is not a breach of any principles 1 to 5, 7 to 10, and 12 if that action is authorised or required by or under law.

Section 7(4) would appear to allow even tertiary legislation (that is, delegated legislation other than regulations) to override the named principles. This is apparently so despite the fact that tertiary legislation is often not subject to disallowance or to other controls which attach to traditional regulations.

11.29 The complexity of these provisions is undesirable, and we think they need redrafting. It is not clear to us why principles 6 and 11 are singled out for special treatment. The provisions also raise some real questions of principle. In general, delegated legislation should not prevail over an Act of Parliament. One can see why it may be undesirable to disturb provisions already in force, but we would prefer that for the future delegated legislation should only be able to derogate from the principles in the Privacy Act if the particular empowering Act of Parliament clearly so provides. We also believe that in cases where that is to be permitted, the delegated legislation should normally be in the form of regulations, so that they come under the scrutiny of the Regulations Review Committee, and are subject to disallowance. Much of this could be achieved by amendments to the current section 7; the Legislation Advisory Committee Guidelines could also usefully contain guidance on the matter.

11.30 We have also considered whether one of the functions of the Privacy Commissioner should be to make complaints to the Regulations Review Committee if she considers any regulations to be objectionable on the basis that they create an undue infringement on privacy rights. One of the functions of the Privacy Commissioner is to examine any *proposed* legislation (including subordinate legislation) and report to the responsible Minister;[899] however, this does not extend to examining subordinate legislation that has been passed. Nevertheless, we think that other functions are broad enough to cover complaints to the Regulations Review Committee, such as the function to make public statements in relation to any matter affecting the privacy of the individual,[900] to make suggestions to any person in relation to any matter that concerns the need for, or the desirability of action by that person in the interests of the privacy of

899 Privacy Act 1993, s 13(1)(o).

900 Privacy Act 1993, s 13(1)(h).

the individual,[901] and to inquire generally into any matter, including any enactment or law if it appears to the Commissioner that the privacy of the individual is being, or may be infringed thereby.[902]

Q127 What presumptions or mechanisms should there be for clarifying the relationship between the Privacy Act and other legislation?

Q128 Should section 7 be redrafted to ensure that future delegated legislation does not override the Privacy Act except insofar as the empowering Act clearly so authorises?

Interaction of common law with the Privacy Act

11.31 Another issue we have considered is the potential for the common law to intersect with the Privacy Act. Specifically, we have considered whether (i) privacy protective doctrines established by the common law, such as breach of confidence and the privacy tort in *Hosking v Runting*, potentially intersect with the Privacy Act; and (ii) whether the common law can establish doctrines that may operate as additional exceptions to the principles (for example, principles of procedural fairness, or exceptions to a duty of confidentiality).[903]

11.32 Where the common law establishes privacy protective doctrines such as the privacy tort in *Hosking v Runting*, these essentially operate in parallel with the privacy principles, with common law doctrines being applied within the jurisdiction of the courts, while the privacy principles are applied within the jurisdiction of the Privacy Commissioner and the Human Rights Review Tribunal.

11.33 Whether any common law exceptions to the principles are effective in the Privacy Act jurisdiction depends on section 7 of the Privacy Act. Section 7 does not defer to the common law in relation to principles 6 and 11.[904] The common law "public concern" exception to non-disclosure has effectively been substituted in principle 11 with enumerated exceptions (e) and (f), and, for purposes of principle 6, is reflected in sections 27 to 29 of the Privacy Act.

11.34 In the case of the other privacy principles, section 7(4) provides that an action will not breach those principles if it is "authorised or required by law". This would seem broad enough to cover the common law.[905] However, there would

901 Privacy Act 1993, s 13(1)(k).

902 Privacy Act 1993, s 13(1)(m).

903 See discussion in Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 16.20–16.71. See also Office of the Privacy Commissioner *Interaction with Other Laws: Review of the Privacy Act 1993 Discussion Paper 10* (Wellington, 1997) 6–7.

904 Section 7(1) deals with "enactments", defined as Acts of Parliament or regulations. See Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) PVA 7.3 (last updated 2007).

905 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) PVA 7.5 (last updated 2007). See *QKB & NSN v Commissioner of Police and Chief Executive, Department of Child Youth and Family Services* (4 October 2006) HRRT Decision No 38/06, summarised in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) HRRT 140 (last updated 2007), where it was argued that the common law principles of witness immunity should exclude liability for breach of principle 8; however the Tribunal did not need to determine that particular issue.

seem to be very few common law rules that would "authorise or require" actions that are in breach of the privacy principles that are not already covered as exceptions to the principles, and section 7(4) would seem to be a "belt and braces" type of provision. Another factor reducing any potential significance of the common law on the principles is the essentially exclusive jurisdiction of the Privacy Commissioner and the HRRT over Privacy Act matters, subject to appeal rights to the courts.[906]

11.35 We note that where a privacy complaint is the subject of proceedings before the Human Rights Review Tribunal, the onus of proving that conduct that is an interference with the privacy of an individual is excused on the basis of a common law exception to the principles left open by section 7(4), would lie on the defendant.[907]

Q129 Do you have any comments about the interaction of the privacy principles with the common law?

OFFICIAL INFORMATION STATUTES

11.36 There are significant linkages and connections between the Privacy Act and the official information statutes. One view of the statutory landscape is that the three statutes[908] can be viewed as complementary components of the same overall statutory scheme. The Official Information Act 1982 (OIA), predating the Privacy Act by 11 years, governs the availability of information (including personal information) held by government agencies and certain public bodies such as school boards of trustees and universities. Requests for information can be made by a broad range of requesters, indeed by any person in New Zealand, or by a body corporate in or carrying on business in New Zealand.[909]

11.37 The Act operates on a principle of openness, but nevertheless contains an important statutory recognition of the importance of the privacy of the individual in the context of official information. The purposes of the OIA are thus stated in section 4 (emphasis added):

> **Purposes**
>
> The purposes of this Act are, consistently with the principle of the Executive Government's responsibility to Parliament, –
>
> (a) 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, –

906 Privacy Act 1993, Part 8. See also Privacy Act, s 11(2) that confirms that the principles do not confer rights that are enforceable in the courts (except principle 6(1)).

907 Privacy Act 1993, s 87.

908 The Privacy Act 1993, the Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987. The Local Government Official Information and Meetings Act 1987 contains parallel provisions to the OIA in relation to official information held by local authorities. While this chapter refers specifically to the Official Information Act, it should be noted that issues raised are also relevant to the Local Government Official Information and Meetings Act.

909 Official Information Act 1982, s 12(1).

and thereby to enhance respect for the law and to promote the good government of New Zealand:

(b) to provide for proper access by each person to official information relating to that person:

(c) to protect official information to the extent consistent with the public interest and the preservation of personal privacy.

There is thus an obvious linkage between the OIA and the Privacy Act.[910]

11.38 The Law Commission is undertaking a separate general review of the OIA.[911] Final recommendations on the relationship between the Acts will not be made until the completion of the OIA review, to ensure a balanced perspective. But it will be helpful to raise the main issues in outline now, and seek preliminary views on them.

The disclosure provisions: comparisons

11.39 Section 9 of the OIA provides:

Other reasons for withholding official information

(1) Where this section applies, good reason for withholding official information exists, for thepurposes of section 5, unless, in the circumstances of the particular case, the withholding ofthat information is outweighed by other considerations which render it desirable, in the publicinterest, to make the information available.

(2) Subject to sections 6, 7, 10 and 18, this section applies if, and only if, the withholding of theinformation is necessary to –

(a) protect the privacy of natural persons, including that of deceased natural persons

This should be contrasted with principle 11 of the Privacy Act which provides:

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,

(a) that the purpose of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary –

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

910 See Judge Anand Satyanand "Interface Between the Official Information and Privacy Acts" (International Symposium on Freedom of Information and Privacy, Auckland, 28 March 2002).

911 New Zealand Law Commission *Statement of Intent 2009–2010* (Wellington, 2009) 29.

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to –

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information –

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under section 54.

We note the following matters which emerge when the two provisions are compared.

The concept of privacy

11.40 It is clear that in at least one respect the concepts of privacy in the two Acts do not coincide: the OIA is concerned to protect the privacy of the deceased as well as the living; the Privacy Act is concerned only with the privacy of the living. But there may be other points of difference. For example, the Privacy Act is concerned only with *personal information*; the OIA concept of privacy may possibly extend to some aspects of spatial privacy as well (such for example as where the provision of information could lead to the invasion of the privacy of a person by, perhaps, a former domestic partner).[912] It may also be that different thresholds of harm or damage are appropriate in the two different contexts.

The public interest override

11.41 In the OIA the privacy interest can be overridden by the "public interest" in disclosure. "Public interest" is not defined, thus allowing a deal of flexibility to accommodate the facts and circumstances of each individual case. This public interest override is of course is not confined to privacy; it applies to all the withholding grounds in section 9.

11.42 On the other hand, principle 11 spells out in its exceptions a number of specific heads of public interest. It provides more guidance, yet takes the risk, as lists of specifics always do, that there may be important aspects which it has omitted to include. It lacks the flexibility of the OIA version.

912 Ian Eagles, Michael Taggart and Grant Liddell *Freedom of Information in New Zealand* (Oxford University Press, Auckland, 1992) 252.

Possibilities for closer alignment

11.43 The differences between the relevant provisions of the two Acts, coupled with the fact that the two Acts start with different presumptions, (the one of disclosure, the other of non-disclosure) can create confusion. When matters reach the Ombudsmen under the OIA, the Ombudsmen are required to consult the Privacy Commissioner in cases where the privacy withholding ground is relied on. We understand that in such cases a solution is usually arrived at simply and seamlessly. But most matters do not reach that point, and agencies and persons who have to operate the legislation in practice do not always find it so easy. We believe it would be helpful if the two Acts were more closely aligned.

11.44 In an earlier review,[913] the Privacy Commissioner raised the possibility of the OIA having more detailed criteria as to what constitutes an unwarranted interference with privacy.

11.45 In examining approaches taken in other countries, we note that in some cases:

- the privacy aspect of the OIA withholding ground refers to, and is more closely aligned with, the relevant privacy statute; and
- more guidance is offered as to the operation of the public interest balancing aspect of the OIA mechanism.

11.46 The interrelationship between the UK's Data Protection Act 1998 and Freedom of Information Act 2000 (FOIA) is an example of seamless consistency between the privacy statute and the freedom of information statute. Section 40 of the FOIA sets out an exemption from the right to know if the information requested is personal information protected by the Data Protection Act. If the requested information under the FOIA is someone else's personal information, the information attracts an absolute exemption if disclosure would breach one of the DPA data protection principles. Because the exemption is absolute, there is then no additional public interest test to consider.[914]

11.47 Under section 41 of the Australian Freedom of Information Act (FOIA) 1982, a document is exempt if disclosure would involve the unreasonable disclosure of personal information about any person (including a deceased person).[915] The ALRC has suggested that the relationship between the Australian FOI and Privacy Acts should be clarified, and has proposed that a document should be

913 Office of the Privacy Commissioner *Interaction with Other Laws: Review of the Privacy Act 1993 Discussion Paper 10* (Wellington, 1997) 13. See also Information Authority *Report of the Information Authority on the Subject of Collection and Use of Personal Information* (Wellington, 1988) 12, recommending an amendment to the OIA which expands on the public interest considerations inherent in sections 9(1) and 9(2)(a) "to give guidance to holders of sensitive personal information, as well as users of the OIA, on matters that should be weighed when considering there is a public interest in releasing information that might invade the privacy of a natural person."

914 Information Commissioner's Office (UK) *Freedom of Information Act, Environmental Information Regulations: The exemption for personal information* (London, 2008).

915 There is a requirement, where practicable, to provide the applicant with access to edited information from which the exempt matter has been deleted: Freedom of Information Act 1982 (Cth), s 22.

exempt under the FOIA if it contains personal information, disclosure would be a breach of the use and disclosure privacy principle, and disclosure would not, on balance, be in the public interest.[916]

11.48 Another model is the British Columbia Freedom of Information and Protection of Privacy Act 1992 which lists circumstances in which disclosure is presumed to be an unreasonable invasion of privacy such as medical history, eligibility for income assistance, racial or ethnic origin, sexual orientation or religious or political beliefs.[917] It also lists circumstances in which disclosure is not an unreasonable invasion of privacy, including information about a person's position or remuneration as an employee of a public body.[918]

11.49 A question is raised, tentatively at this stage (because a definitive answer must await the completion of the OIA review) whether there should be a closer alignment of the two New Zealand Acts by either or both:

- defining the privacy withholding ground in the OIA by reference to principle 11 in the Privacy Act; and
- being more specific about the respects in which the "public interest" override in the OIA aligns with, or is wider than, the exceptions in privacy principle 11.

In examining these questions, we must be mindful that the OIA relates only to information held by government agencies, and that different considerations apply to them than apply to the private sector. We must also keep in mind that privacy is only one withholding ground under the OIA, and that "public interest" is a general override which applies to other grounds as well.

Q130 What are your views on whether there should be closer alignment of the tests for disclosure of personal information under the Official Information Act and the Privacy Act?

Making the OIA override explicit

11.50 Whatever is done in response to the issues discussed above, we wonder whether it should be made clear in the legislation that, in relation to the release of official information, the OIA overrides the Privacy Act. This is well known to those experienced in the area, but it is not explicit on the face of either statute, and can cause confusion for the less experienced.

916 The Australian Law Reform Commission made a recommendation along these lines in *Open Government: A Review of the Federal Freedom of Information Act* (ALRC R77, Sydney, 1995) recommendation 59. More recently the proposal was outlined in Australian Law Reform Commission *Review of Privacy* (ARLC DP72, Sydney, 2007) Proposal 12-2. Pending the Commission's intended review of the FOIA, however the terms of reference for this review were subsequently revoked. See Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 15.10–15.11.

917 Freedom of Information and Protection of Privacy Act 1992 (BC), s 22(3)(a), (c) and (h).

918 Freedom of Information and Protection of Privacy Act 1992 (BC), s 22(4)(a), (c) and (h).

11.51 In consultation with the Office of the Privacy Commissioner during the present review, we were advised that while the interface is generally easy, and mostly the process works well, it is acknowledged that for users of the legislation who are not familiar with its intricacies (such as schools, for example)[919] it is not easy to understand the statutory interface.

11.52 There may be some merit in making this statutory override explicit. As noted by the Privacy Commissioner,[920] the Privacy of Information Bill (the precursor to the Act) originally contained an exemption to its non-disclosure principle for disclosures made under the OIA. A published list of statutory overrides would be another way to make the override express.

Q131 Should the Privacy Act's deferral to the OIA be made explicit?

Lack of complaint or review processes for disclosures of personal information under the OIA

11.53 It is possible that sometimes a release of personal information under the OIA may take inadequate account of the privacy interest of an individual. In other words, sometimes personal information may be released without the privacy withholding ground in section 9(2)(a) of the OIA having been adequately addressed.[921] The question is whether an individual whose privacy is thus breached should have any redress. This question cannot be looked at in isolation: there is a broader question of whether a remedy should be available to anyone who suffers detriment because insufficient attention has been paid to any of the withholding grounds under the OIA (prejudice to commercial position, or an obligation of confidence are two further examples). The Danks Committee which recommended the enactment of the OIA did not propose a complaints mechanism for such releases.[922]

11.54 Under the Ombudsmen Act 1975 a function of the Ombudsmen is to review matters of administration affecting any person in their personal capacity, and it is possible that the Ombudsmen might be able, under this function, to review an allegedly improper release of information.[923]

---

919 Kathryn Dalziel *Privacy in Schools: a Guide to the Privacy Act for Principals, Teachers and Boards of Trustees* (Office of the Privacy Commissioner, Wellington, 2009) 24.

920 *Necessary and Desirable* paras 2.15.18–2.15.19

921 Official Information Act 1982, s 9(2)(c).

922 Committee on Official Information *Towards Open Government* (Supplementary Report, Wellington, 1981) para 2.22. Section 28 of the OIA provides that it is a function of the Ombudsman to review decisions under Part 2 of the OIA, but these are limited to agency decisions to withhold information or impose conditions on release.

923 Ombudsmen Act 1975, ss 13(1) and 22(1). See also *Laws of New Zealand* (Butterworths, Wellington, 1992) Administrative Law (11) Ombudsmen para 227, fn 1, noting that "matter of administration" has been held to encompass everything other than legislative or judicial activities, citing *British Columbia Development Corp v Friedman* (1984) DLR (4th) 129. There may also be other avenues of complaint such as civil action and judicial review, but these are costly. See for example, *Veitch v New Zealand Police* (20–21 May 2009) HC WN CIV-2009-485-960 Mallon J, where the plaintiff obtained an interim injunction to restrain the publication of information about him obtained by the media from the Police under the OIA. See also Ian Eagles, Michael Taggart and Grant Liddell *Freedom of Information in New Zealand* (Oxford University Press, Auckland, 1992) 620–622.

11.55 As far as privacy is specifically concerned, it has been held that a complaint cannot be made to the Privacy Commissioner under the Privacy Act on the ground that the OIA decision-making process was defective in that it failed to take adequate account of privacy. In *Director of Human Rights Proceedings v Police*[924] the High Court took the view that if the Privacy Act was intended to confer a jurisdiction on the Human Rights Review Tribunal to review the quality of an agency's exercise of its discretion under the OIA, it would have said so expressly.

11.56 The question is: given that a decision under the OIA to withhold information is expressly reviewable, should this be balanced by a right to review a decision to release? It should be noted that in Australia, the Freedom of Information Act allows for remedies in this situation, and indeed provides that a person can apply to the Administrative Appeals Tribunal for a review of a decision to release their personal information in response to a request.[925]

11.57 We shall be considering the issue more generally in our review of the OIA, but would at this point welcome any comments, particularly in the context of the privacy withholding ground.

11.58 Possible options for New Zealand might include:

- providing the Ombudsmen with the express power to review decisions to release; and
- extending the Privacy Commissioner's complaints process to OIA releases of personal information.

A relevant factor will be the extent to which the very existence of a complaints process would impact unduly on the OIA regime by inhibiting the release of official information.

Q132 Should consideration be given to a specific right of review or complaints process for those affected by the release of personal information under the OIA?

Consultation and notification

11.59 A related question is whether disclosure under the OIA should be preceded by notification to any person whose personal information is or is proposed to be disclosed. While the Ombudsmen have indicated that it is good practice to consult those affected before release,[926] consultation is not mandatory under the OIA. In an earlier review, the Privacy Commissioner raised the possibility of an obligation to consult the individual concerned before releasing personal information to third parties, as is the Canadian approach.[927] In Australia, the

924 *Director of Human Rights Proceedings v Police* (14 August 2008) HC WN CIV-2007-409-002984.

925 Office of the Ombudsmen *How the Official Information Legislation Works* www.ombudsmen.parliament.nz (accessed 21 January 2009) chapter 4.1, 4.3.

926 Office of the Ombudsmen *How the Official Information Legislation Works* www.ombudsmen.parliament.nz (accessed 21 January 2009) chapters 4.1, 4.3.

927 Office of the Privacy Commissioner *Interaction with Other Laws* – Review of the Privacy Act 1993 Discussion Paper 10 (Wellington, 1997) 13. See also the Australian provision: Freedom of Information Act 1982 (Cth), s 27A.

FOIA contains a duty to consult with the information subject if it appears that he or she might reasonably wish to contend that the document is exempt from disclosure, but only to the extent that it is reasonably practicable to do so having regard to all the circumstances, including time limits for processing requests.

11.60 While we see merit in a requirement of consultation, it has two very obvious drawbacks. One is that it will slow down the OIA process, where delay is already a significant issue. Another is that it would impose another, and very heavy, burden on agencies, many of whom are already under pressure handling OIA requests.

11.61 The ALRC considered this problem and recommended that guidelines on consultation should advise agencies to suggest to applicants that the consent of the person whose information is being requested will expedite the request, and that agencies should clarify, to the extent it is unclear, whether third party personal information is required under the request.[928]

Q133 Should consideration be given to formalising a consultation process between the public agency holding personal information and a person who may be affected by the release of that information under the OIA?

OIA requests between public sector agencies

11.62 One fundamental question relating to the interaction between the Privacy Act and the OIA is whether requests by government agencies for personal information held by other government agencies are subject to the Privacy Act (privacy principle 11) or the OIA. The question is of some significance: if the OIA overrides the Privacy Act in this context, then government agencies can avoid the limits on disclosure in privacy principle 11, provided that there is a sufficient public interest in disclosure that outweighs the relevant privacy interest. It could be a justification for information sharing between agencies.

11.63 While the OIA definition of a "person" is broad and would not seem to preclude OIA requests by government agencies, our initial view is that the OIA is not the intended or appropriate framework for inter-agency requests for personal information. It could be questioned whether inter-agency access to official information is consistent with the purposes of the OIA, which are primarily about making information available to citizens, rather than sharing information within government.[929] We are also concerned that government agencies using the OIA to obtain personal information could potentially circumvent Privacy Act restrictions on information-sharing.[930] Another consequence of this approach is that it would involve the Ombudsmen in disputes over non-disclosure between government agencies, which would represent a departure from the Ombudsmen's usual role as an arbiter of disputes between government and citizens in relation to access to official information.

928 Australian Law Reform Commission *Open Government: A Review of the Federal Freedom of Information Act* (ALRC R77, Sydney, 1995) recommendation 62.

929 See above para 11.37.

930 See chapter 10. In relation to data matching (discussed in chapter 9), section 109 of the Privacy Act confirms that the OIA cannot be used by public sector agencies to avoid the Privacy Act limits.

11.64 In *QKB & NSN v Commissioner of Police and Chief Executive, Department of Child Youth and Family Services*[931] one question was whether a disclosure by the Police to Child Youth and Family Services for the compilation of a report under section 29 of the Guardianship Act was made under the Privacy Act or the OIA. The Tribunal found that it was not clear on what statutory basis the information was collected or disclosed and noted:[932]

> There are some factors that support the view that, if the parties had thought about the matter at the time, they might have regarded the request as coming under the Official Information Act rather than the Privacy Act….On the other hand, the fact that the parties were careful to obtain the consent of the plaintiffs to the release of the information suggests that they might not have seen the request as falling under the Official Information Act had they given the matter any thought (or, at least, that they recognised that privacy issues were at stake).

The Police submitted that the request for information from Child Youth and Family Services should be treated by the Tribunal as an OIA request; however, the Tribunal proceeded on the basis that the Privacy Act applied but found no breaches of principles 8 or 11 or any interference with the plaintiffs' privacy under section 66 of the Privacy Act. So there is a lack of clarity about whether public sector agencies can make requests to each other for information about citizens under the OIA.

11.65 Nevertheless, many agencies and organisations are subject to the OIA. It may be appropriate for some of them to seek information from government under the OIA: school boards of trustees or Fish and Game Councils, for example. There is no reason in logic or policy why, just because an organisation is subject to disclosure of information held by it, it should be barred from seeking information itself. Our concern centres rather on core public service departments and ministries which hold large amounts of information about individuals using the OIA to get information from each other in the absence of any protocols or approvals. We deal with the very important question of information sharing in chapter 10 of this Issues Paper.

11.66 Our tentative view is that the OIA should not be used by public service departments and ministries to acquire personal information about citizens from each other. If this view is correct, the question is whether this would be best made clear by an amendment to the OIA, or whether a Cabinet direction might be sufficient. In either case there may be a difficult boundary issue as to which agencies the prohibition should apply to.

Q134 Should the OIA be able to be used by government agencies to obtain from each other information about individuals? If not, how should such a limitation be given effect?

931 *QKB & NSN v Commissioner of Police and Chief Executive, Department of Child Youth and Family Services* (4 October 2006) HRRT Decision No 38/06, summarised in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) HRRT 140 (last updated 2007).

932 *QKB & NSN v Commissioner of Police and Chief Executive, Department of Child Youth and Family Services* (4 October 2006) HRRT Decision No 38/06, para 27, summarised in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) HRRT 140 (last updated 2007).

Combining the Privacy Act and the OIA

11.67 We note that the ALRC has considered the option of combining the Australian Privacy Act and Freedom of Information Act, and also the option of combining these two Acts with the Archives Act into a single Act. However, there was little support for this option and it was decided not to disturb the current legislative framework for insufficient benefit.[933]

11.68 Our initial view is that similarly there is unlikely to be sufficient justification for altering the well entrenched New Zealand legislative framework.

> Q135 Should consideration be given to combining all, or any parts, of the Privacy Act, the Official Information Act and the Public Records Act?

Regulation of Privacy and Freedom of Information

11.69 A further question is whether there might be a merger, or at least co-location, of regulators. The ALRC has considered the option of having the same regulator administer the Privacy Act and the Freedom of Information Act but there was little support for the proposal and the Commission did not recommend a single regulator.[934]

11.70 However, the Australian Government has introduced a Bill[935] to implement its 2007 election policy to restructure information regulation. The role of the Privacy Commissioner is to be preserved, a Freedom of Information Commissioner is to be appointed,[936] and these two Commissioners are to be co-located. A new Office of Information Commissioner would be created to act as a whole-of-government clearing house for complaints, oversight, advice and reporting (in an Annual Report) for freedom of information and privacy matters.

11.71 In New South Wales, the Ombudsman in 1989 proposed an Information Commissioner as a central independent agency overseeing freedom of information and suggested that consideration be given to making the Information Commissioner responsible for oversight of privacy as well.[937] The Government Information (Information Commissioner) Act 2009 (NSW) establishes an Information Commissioner, but with functions relating to freedom of information only.

933 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 13.28–13.29.

934 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 13.30–13.33.

935 Information Commissioner Bill 2009. The Bill as introduced follows a consultation draft.

936 The FOI Commissioner is to precede the Administrative Appeals Tribunal appeals process in the FOI review process and to take on most of the Commonwealth Ombudsman's role in investigating delays and complaints about FOI.

937 New South Wales Ombudsman *Opening Up Government: Review of the Freedom of Information Act 1989* (Sydney, 2009) recommendations 83–88. For the response of the New South Wales Law Reform Commission see paras 36–46.

11.72 In the United Kingdom, the Information Commissioner has responsibility for both the Data Protection Act and the Freedom of Information Act.

11.73 In New Zealand, an Information Authority was established for a five year period (1983–1988) under Part 6 of the OIA (now repealed).[938] The Information Authority published a number of reports on the collection and use of personal information,[939] which had an influence on the drafting of the Privacy of Information Bill[940] (the precursor to the Privacy Act 1993), and had a range of functions and powers including to review the working of the OIA and the manner in which official information is supplied,[941] as well as certain functions in respect of personal information.[942] We propose to consider the role of the former Information Authority in our separate review of the Official Information Act.

11.74 In the meantime, we are interested in views on options for an information regulator spanning both privacy and freedom of information.[943] This could involve looking at the proposed Australian model with an Information Commissioner presiding over the Privacy Commissioner and Freedom of Information Commissioner, or the functions of the Privacy Commissioner and the freedom of information functions of the Ombudsmen being subsumed in one Information Commissioner, as per the UK model.

Q136 Do you have any preliminary views on umbrella regulation of privacy and freedom of information?

Access to personal information

11.75 When the OIA was passed it conferred an entitlement on both natural persons and legal persons to access personal information about them held by an agency subject to the Act. When the Privacy Act came into force in 1993 it conferred on a natural persons the right to access personal information about them held by both private and public agencies. In respect of public agencies subject to the OIA, this access right of natural persons was removed from the OIA to the Privacy Act.

938 Ian Eagles, Michael Taggart and Grant Liddell *Freedom of Information in New Zealand* (Oxford University Press, Auckland, 1992) 35.

939 Information Authority *Personal Information and the Official Information Act: An Examination of the Issues* (Wellington, 1985); *Personal Information and the OOfficial Information Act: Recommendations for Reform* (Wellington, 1987); *Report of the Information Authority on the Subject of Collection and Use of Personal Information* (Wellington, 1988).

940 *Necessary and Desirable* 23.

941 Official Information Act 1982, s 38(2)(a) (now repealed).

942 Official Information Act 1982, s 39 (now repealed).

943 Note that this issue will be considered primarily in the Law Commission's review of the OIA.

11.76 The present position is thus somewhat fragmented.

- Natural persons have access rights to personal information about them against both private and public sector agencies under the Privacy Act. Complaints against refusal of access are made to the Privacy Commissioner.
- Corporations have access rights against public sector agencies under the OIA. Complaints against refusal of access are made to the Ombudsmen.
- Corporations have no access rights against private sector organisations. (We ask in chapter 3 whether they should.)

Fragmentation is inevitable as long as there is a distinction between the public and private sectors, and between natural and legal persons.

11.77 The only question for this chapter is whether the current division between the Acts, and the two complaints authorities, is the right one, or whether the access rights of natural persons against public sector agencies should revert back to the OIA. That would have the advantage that the Ombudsmen would have the jurisdiction over all access complaints against public sector agencies. On the other hand, the present position means that the Privacy Commissioner has jurisdiction over access to all personal information wherever it is held, and can facilitate uniform practices and expectations in relation to privacy.

11.78 It seems to us that there is not a strong case for disturbing the status quo, but we would be interested in views.

Q137 Do you have views about the current division of access rights between the Privacy Act and the OIA?

PUBLIC RECORDS ACT

11.79 The Public Records Act 2005 (PRA) provides for the transfer to the Archives of public records. The scheme of the Act, so far as is relevant to our inquiry, is that every public office must transfer to the possession of Archives New Zealand, or another approved repository, public records which are 25 years old.[944] There is provision for deferral in appropriate cases. When records are about to be transferred to the Archives, the administrative head of the relevant public office must classify the records as either open access records or restricted access records. In making that distinction the head must consider whether:[945]

(a) there are good reasons to restrict public access to the public record, having regard to any relevant standard or advice issued by the Chief Archivist; or

(b) another enactment requires the public record to be withheld from public access.

11.80 If neither of those two criteria are satisfied, the work must be classified as open access.[946] If access is to be restricted, the head of the relevant public office must consult with the Chief Archivist as to whether there should be access on conditions.[947] If records are classified as open access, the records must be made available to members of the public.[948] The Chief Archivist has power to issue

944 Public Records Act 2005, s 21(1).

945 Public Records Act 2005, s 44(1)(a)(b).

946 Public Records Act 2005, s 44(2).

947 Public Records Act 2005, s 44(3).

948 Public Records Act 2005, s 47.

standards for, among other things, the provision of access to public records.[949] He or she can also authorise the disposal of public records, including their destruction.[950]

11.81 Given that some public records contain personal information, there is a question of the interface between the PRA, the Privacy Act 1993 and the privacy ground for withholding information in the OIA. We believe it would be desirable for the relationship between these three pieces of legislation to be clarified in one or all of them. The following areas, we believe, merit discussion.

Transfer to the Archives

11.82 Section 21(1) of the PRA mandates transfer to Archives New Zealand or another approved repository of "public records".[951] "Public record" is defined to mean "a record or class of records, in any form, in whole or in part, created or received… by a public office in the conduct of its affairs."

11.83 Section 21(1) applies to all public records unless they are to be destroyed in accordance with the Act, or there is an agreement that they be transferred earlier than the 25 years, or the transfer is deferred under section 22. On the face of it, this could lead to the compulsory archiving of unmanageable volumes of material, including personal information about employees and others. There could in theory be a serious privacy issue. In fact, a very small proportion of records (about 6 per cent) are actually transferred to the Archives. We understand that the purpose section of the PRA is used to determine where the boundary lies.

11.84 Section 3(c)(ii) provides that a purpose of the PRA is to enable the government to be held accountable by:

> providing for the preservation of, and public access to, records of long-term value.

Section 3(f) provides that a further purpose is

> through the systematic creation and preservation of public archives and local authority archives, to enhance the accessibility of records that are relevant to the historical and cultural heritage of New Zealand and to New Zealanders' sense of their national identity.

11.85 If this is a correct approach, it means that the only material which will be transferred to Archives is that which has value in the senses specified in those paragraphs – material, in fact, which is of public interest. Much material containing private personal information would not qualify, and thus would probably not be transferred to Archives at all. It is unusual for a purpose section to carry such substantive weight. We would prefer the tests for the types of record which have to be archived to be spelled out in section 21, rather than being left to the purpose section.

949 Public Records Act 2005, s 27.

950 Public Records Act 2005, s 20.

951 Public Records Act 2005, s 4.

The criteria for open and restricted access

11.86 Once a decision has been made to transfer material to the Archives, a decision must be made on the question of open or restricted access. If another enactment requires withholding of the material it will be placed on restricted access: the Adoption Act 1955 and the Criminal Records (Clean Slate) Act 2004 would be examples. It is an open question whether principle 11 of the Privacy Act (the disclosure principle) could ever apply in this context. It is certainly "another enactment" but the question is whether, as a principle, it "requires" access to be restricted.

11.87 The other ground for a restricted classification is if there are "good reasons to restrict access" having regard to "any relevant standard or advice issued by the Chief Archivist". Guidelines issued by the Chief Archivist state two grounds relevant to privacy:[952]

- to prevent the disclosure of sensitive personal information; and
- to prevent the disclosure of highly sensitive personal information.

These grounds imply a higher threshold than the Privacy Act's protection of personal information which does not depend on the level of sensitivity of the information. Perhaps the element of public interest in the information justifies the discrepancy, but discrepancy it is.

11.88 The guidelines also give examples of types of records and suggested restriction periods, for example:

- Detailed employment records, disciplinary case files, applications for financial assistance: **70 years, then open**
- Child welfare files, medical records, probation records, police incidence and offences files: **100 years, then open**
- Information gathered with explicit or implicit undertaking of confidence, such as survey forms: **30 years, then review**
- Sensitive information regarding people, places, or cultural practices that would not normally be made public: **70 years, then review.**

11.89 Thus the PRA regime for deciding on the type of access is not on all fours with the Privacy Act and the OIA. We think it would avoid confusion if the relationships between the Acts at this decision-making stage could be clarified by express provision in the Public Records Act. It might, for instance, be provided that any Guidelines laid down by the Chief Archivist must take into account the provisions of these other two Acts.

952 Archives New Zealand *Making Access Decisions under the Public Records Act* (Wellington, 2005).

Open access

11.90 Once access is open, the right of an individual to access information about himself or herself under privacy principle 6 obviously becomes redundant, as do the reasons for withholding in sections 27–29 of the Privacy Act.

11.91 Likewise, once access is open, the records are available to the public as of right. They do not have to be requested under the OIA. But there is a question whether, if the records contain sensitive personal information, the person concerned has any recourse in respect of the decision to make them open access. There is no express right in the person to ask for the decision to be reviewed, and we wonder whether there should be. It may be that there is already a right to complain to the Ombudsmen under the Ombudsmen Act 1975, or the Privacy Commissioner under the Privacy Act (for breach of principle 11); that could also be spelt out with advantage.

Restricted access

11.92 If access is restricted there is no automatic right to access the work except in accordance with any conditions which may have been imposed at the time of the classification. However, section 44(8) of the PRA effectively provides (albeit by implication), that the OIA and Privacy Act continue to apply to information in the record; it states expressly that it is the controlling public office to which the request for access under those Acts should be made:

> Every controlling public office is responsible for dealing with requests for official information under the Official Information Act 1982 and requests for personal information under the Privacy Act 1993.

To that limited extent, then, the Privacy Act and the OIA have an express place in the PRA. No further provision seems necessary in this matter.

Retention

11.93 Privacy principle 9 provides that an agency shall not keep personal information for longer than is required for the purposes for which the information may lawfully be used. Section 18 of the PRA provides that no person may dispose of public records without the authority of the Chief Archivist, unless the disposal of a public record is required by or under another Act.

11.94 The interaction of these 2 provisions requires clarification, the question being whether privacy principle 9 is a requirement "by or under another Act" for the purposes of section 18 of the PRA. In other words, there is a question of which of the two provisions has precedence.

11.95 We note that the ALRC has recommended a statutory clarification of the precedence of the Archives Act 1983 (Cth) over the data security principle, that is, that the data security principle is not an obligation to destroy personal information that is "required by law."[953] The ALRC also recommended that the Australian Privacy Commissioner publish guidance about the disposal principle including the interaction between the data destruction requirements and legislative records retention requirements in the Archives Act.[954]

Conclusions

11.96 We think the interrelation between the PRA and the Privacy Act, and also between the PRA and the privacy withholding ground in the OIA, is not as clear as it should be. We believe that clarity would be improved if the Acts referred to each other, and a further attempt was made to secure a "fit" between them.

Q138 Do you have any views about the interrelationship between the Public Records Act and the Privacy Act, and between the Public Records Act and the privacy withholding ground in the OIA? Do you agree that the relationship between the different legislation should be clarified?

Q139 Should remedies be available to a person aggrieved by a decision to place personal information on open access in the Archives? If so, what kind of remedies?

OTHER STATUTES

11.97 There are a range of other statutes that contain specific overrides of the privacy principles. We mention a couple of these and invite comment on any other statutory intersections with the Privacy Act that require clarification.

Health and Disability Commissioner Act 1994

11.98 The Health and Disability Commissioner Act 1994 establishes the office of the Health and Disability Commissioner,[955] a complaints process for consumers of health care or disability services,[956] and an advocacy service.[957] It also provides for the issue of a Code of Health and Disability Services Consumers' Rights.[958]

953 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 28-4(b). The Australian Government has accepted that recommendation.

954 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 21-5. The Australian Government has accepted that recommendation.

955 Health and Disability Commissioner Act 1994, Part 1.

956 Health and Disability Commissioner Act 1994, Part 4.

957 Health and Disability Commissioner Act 1994, Part 3.

958 Health and Disability Commissioner Act 1994, Part 2; Code of Health and Disability Services Consumers' Rights 1996.

11.99 One of the rights of a consumer in the Code is the right to have his or her privacy respected.[959] The definition of "privacy" in the Code excludes matters of privacy that may be the subject of a complaint under the Privacy Act.[960] Thus, there is a clear boundary between the privacy jurisdictions of the Privacy Commissioner and the Health and Disability Commissioner. Essentially, health information privacy falls within the jurisdiction of the Privacy Commissioner, while bodily privacy intrusions relating to health or disability services fall within the jurisdiction of the Health and Disability Commissioner.[961]

11.100 The Health and Disability Commissioner shares jurisdiction with the Chief Human Rights Commissioner in relation to complaints alleging discrimination, with the two Commissioners consulting as to which body should deal with the complaint.[962] In the privacy context, the legislative framework generally establishes separate jurisdiction between the Privacy Commissioner, the Ombudsmen, and the Health and Disability Commissioner.

11.101 The Health and Disability Commissioner has completed his third review of the Health and Disability Commissioner Act and the Code.[963] One of the Commissioner's key recommendations is to amend the Act and the Code to give the Commissioner joint jurisdiction with the Privacy Commissioner in relation to health information privacy. The Commissioner argues that the current split jurisdiction results in a duplication of process and detracts from seeing a complaint in its totality. According to the review, where information privacy is only a minor aspect of a complaint, the Health and Disability Commissioner has to deal with the health information aspect of the complaint in a convoluted manner. In consultation on the review, the Health and Disability Commissioner received 33 submissions in support of the change, while 14 submissions endorsed the status quo.

11.102 The Privacy Commissioner strongly opposed the proposition for joint jurisdiction, arguing that this would add confusion rather than clarity and introduce the potential for differing interpretations of health information privacy under the Privacy Act (including the Health Information Privacy Code) and the Health and Disability Commissioner Act. The Privacy Commissioner raised some alternative options, such as confirming the Health and Disability Commissioner's jurisdiction in relation to breaches of confidentiality. According to the Privacy Commissioner, the current split jurisdiction results in only occasional transfers of complaints between the two Commissioners.

---

959 Code of Health and Disability Services Consumers' Rights 1996, r 2, Right 2.

960 Code of Health and Disability Services Consumers' Rights 1996, r 4.

961 However, the Health and Disability Commissioner has occasionally considered complaints involving disclosure of health information in relation to a breach of the ethical duty of confidentiality in terms of Right 4(2) of the Code of Health and Disability Services Consumers' Rights: "the right to have services provided that comply with legal, professional, ethical and other relevant standards." See Joanna Manning "Review of New Zealand's Health and Disability Commissioner Act and Code of Rights" (2009) 17 JLM 314, 319.

962 Health and Disability Commissioner *Consultation Document: Review of the Health and Disability Commissioner Act 1994 and Code of Health and Disability Services Consumers' Rights* (Wellington, 2008).

963 Health and Disability Commissioner *A Review of the Health and Disability Commissioner Act 1994 and Code of Health and Disability Services Consumers' Rights* (Report to the Minister of Health, Wellington, 2009).

Q140 Do you have any view about the question of jurisdiction for health information privacy as between the Privacy Commissioner and the Health and Disability Commissioner?

Statistics Act 1975

11.103 The Statistics Act overrides the Privacy Act principles in relation to the collection and use of personal information by Statistics New Zealand and other government departments producing official statistics. While on the one hand people are legally required to provide information for official surveys, on the other hand there are strong privacy protections in that the information can only be used for statistical purposes, identifiable information is not to be published or otherwise disclosed (subject to certain exceptions including consent, or where the information is publicly available) and there are specific security requirements, including secrecy obligations of Statistics staff.[964]

11.104 The Privacy Act applies to the use of personal information for statistical purposes by agencies that are not covered by the Statistics Act. Principles 2, 3, 10 and 11 contain exceptions where the information will not be used in a form where the individual concerned is identified or will be used for statistical or research purposes and not published in a form that could reasonably be expected to identify the individual.

Data integration

11.105 Statistics New Zealand has developed a data integration policy where data is linked together from different sources.[965] Privacy considerations include an initial assessment of whether the data integration benefits outweigh privacy concerns and a privacy impact assessment must be carried out. Integrated data must only be used for approved statistical purposes or related research purposes, integrated datasets must be destroyed once the purposes of data integration have been achieved, data integration must not be undertaken in secret and the primary results of data integration must be made publicly available. These protocols have been cited with approval by former Privacy Commissioner Bruce Slane,[966] affirming a suggestion that they could be embedded in a Code of Practice.

Q141 Do you have views about how privacy can be protected in relation to personal information used for statistical purposes?

964 Statistics Act 1975, ss 21, 37 and 37A. See also Statistics New Zealand "Confidentiality of Information Supplied to Statistics New Zealand" www.stats.govt.nz (accessed 6 April 2009).

965 Statistics New Zealand "Data Integration Policy" www.stats.govt.nz (accessed 6 April 2009).

966 Bruce Slane, Privacy Commissioner "Administrative Statistics, Respondent Burden and Privacy" (Address to New Zealand Conference on Database Integration and Linked Employer-Employee Data (DILEED), Wellington, 21–22 March 2002).

Secrecy provisions in statutes

11.106 A number of New Zealand statutes contain secrecy provisions that require officials not to disclose certain types of information.[967] In its recent review, the ALRC concluded that it is appropriate that specific statutes include secrecy provisions designed to protect information and that information protected by secrecy should not be regulated by the Privacy Act. However, the Commission suggested that a privacy impact assessment should be prepared when a secrecy provision is proposed in new legislation that may have a significant impact on the handling of personal information, and that where a secrecy provision regulates personal information it should address how the requirements under the provision interact with the privacy principles.[968] The Commission is now conducting a specific review of secrecy laws in Australia and the way in which secrecy provisions intersect with other laws such as privacy, freedom of information, archiving, whistle-blowing and data-matching.[969]

11.107 In New Zealand, the Privacy Commissioner has previously raised the potential impact of secrecy provisions on personal privacy, particularly on rights of access under principle 6 and has recommended that secrecy provisions should be reviewed to ensure that access rights under principle 6 are not unnecessarily precluded.[970]

11.108 In Q126, we asked whether a published list of statutory provisions that override the privacy principles would be helpful. A list of this sort would include statutory secrecy provisions, and may help both to identify secrecy provisions that intersect with the Privacy Act and any areas of uncertainty. We also invite submissions on whether a review of statutory secrecy provisions would be desirable in New Zealand.

Q142 Is a review of statutory secrecy provisions desirable?

Q143 Does the intersection of any other legislation with the Privacy Act require clarification or review?

967 See, for example, Tax Administration Act 1994, s 81; Serious Fraud Office Act, s 36; Ombudsmen Act 1975, s 21.

968 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 15.120–15.122.

969 Australian Law Reform Commission *Review of Secrecy Laws* (ALRC DP 74, Sydney, 2009).

970 *1st supplement to Necessary and Desirable* recommendation 34A. The Law Commission also discussed aspects of secrecy provisions in its report on stage 3 of this Review: New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, Wellington, 2010) ch 8.

Chapter 12
Law enforcement

12.1 One of the main interests which must be weighed in the balance with the privacy interest is the state's interest in maintenance of the law. So, while law enforcement agencies such as the Police are subject to the Privacy Act, a number of the privacy principles allow for a "maintenance of the law" exception; namely, the collection,[971] access,[972] use,[973] and disclosure[974] principles. In addition to the principles, Part 11 and Schedule 5 of the Privacy Act authorise the sharing of specific personal information that is necessary for the operation of the justice sector, between various public sector agencies including the Police and other law enforcement agencies. The use of unique identifiers by justice sector agencies (including law enforcement agencies) is regulated by the Justice Sector Unique Identifier Code 1998.[975] The Official Information Act governs requests made to law enforcement agencies for official information that may comprise personal information about other people.[976]

12.2 In this chapter we discuss issues with the law enforcement provisions under two main headings:

- substantive and administrative issues relating to requests for access to personal information held by the law enforcement agency about the requester under principle 6; and
- Privacy Act requirements applying to information sharing for law enforcement purposes.

ACCESS REQUESTS

Law enforcement intelligence

12.3 One issue raised is whether people should be able to access "intelligence" about them that is held by a law enforcement agency. Police create profiles of individuals using intelligence and there is concern that police operations may be prejudiced if individuals were made aware of details that have been collected about them by police. The view of the Police is that to be effective, intelligence should not

971 Privacy Act 1993, s 6, principles 2(2)(d)(i) and 3(4)(c)(i).

972 Privacy Act 1993, s 27(1)(c).

973 Privacy Act 1993, s 6, principle10(c)(i).

974 Privacy Act 1993, s 6, principle 11(e)(i).

975 The Justice Sector Unique Identifier Code is a Code of Practice issued under the Privacy Act 1993, Part 6.

976 The interaction between the OIA and the Privacy Act is discussed in chapter 11. One issue is whether law enforcement agencies can themselves use the Official Information Act to request official information about people from other government agencies.

be disclosed to the person concerned. On the other hand, it is argued that individuals who are targeted by police surveillance have the right to know what information is held about them by the authorities, especially when those individuals are not involved in criminal offending. The collection of intelligence about individuals involved in protest groups by the police has attracted controversy both in New Zealand[977] and in the United Kingdom.[978]

12.4 Part 4 of the Privacy Act covers good reasons for refusing access to personal information, one of which is "prejudice to the maintenance of the law, including the prevention, investigation, and detection of offences and the right to a fair trial".[979] This ground is used to withhold informant identity information (where there is reason to believe that disclosure of informant identity would cause informant information to dry up), and to withhold personal information about the target of an investigation pending completion of the investigation.[980] Section 32 authorises an agency to give a "neither confirm nor deny" notice in response to an access request where this ground for refusing access is established.

12.5 In our view, the maintenance of law exception, together with the ability to neither confirm nor deny in section 32, generally provides a sufficient balance between law enforcement and privacy interests in relation to the release of personal information to the person concerned. It would not be appropriate in our view to create a specific exemption for intelligence information from the operation of principle 6, or, more generally, to exclude the intelligence gathering activities of law enforcement agencies from the operation of the Privacy Act.[981]

12.6 We note that the ALRC has considered whether the law enforcement exceptions to the privacy principles are adequate to accommodate operational issues or whether a special exemption is required (such as in New South Wales and Victoria where law enforcement agencies enjoy exemptions from state privacy legislation).[982] The ALRC concluded that the exceptions to the principles are generally adequate to accommodate the functions and operations of law enforcement agencies and concluded that no special exemption from the Privacy Act is required.[983]

977 "The Activist who Turned Police Informer"; "Who the Police Were Spying On"; "How Gilchrist Was Found"; "Anti-Terror Squad Spies on Protest Groups" (14 December 2008) *Sunday Star-Times*; Martin Kay "Collins Demands Spy Facts" (15 December 2008) *Dominion Post* Wellington; Lincoln Tan "Chief of Police Called In Over Spies" (15 December 2008) *New Zealand Herald* Auckland.

978 Paul Lewis and Marc Vallée "Revealed: police databank on thousands of protesters" (6 March 2009) *The Guardian* London.

979 Privacy Act 1993, s 27(1)(c).

980 *Necessary and Desirable* paras 4.2.8–4.2.12.

981 While "intelligence agencies" enjoy a Privacy Act exemption under s 57, that exemption does not extend to principle 6 (access) or principle 7 (correction). There is however a special complaints procedure (section 81). See further chapter 5.

982 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 37.73–37.113.

983 Except in the case of the Australian Crime Commission responsible for investigating organised crime and the Integrity Commissioner responsible for investigating corruption; it was considered that these bodies have a separate system of oversight and accountability including ministerial oversight.

Formulation of the "maintenance of law" exception to the access principle

Other jurisdictions

12.7 We note that the "maintenance of law" exception to the access principle is spelt out in more detail in the British Columbia and Australian privacy legislation than the maintenance of law exception to New Zealand's principle 6. There are 12 law enforcement-related reasons for which access may be denied under the British Columbia Freedom of Information and Protection of Privacy Act, including where disclosure could reasonably be expected to:

- harm the effectiveness of investigative techniques and procedures currently used or likely to be used, in law enforcement;
- reveal the identity of a confidential source of law enforcement information;
- reveal any information relating to or used in the exercise of prosecutorial discretion;
- deprive a person of the right to a fair trial or impartial adjudication;
- reveal a record that has been confiscated by a peace officer in accordance with an enactment; or
- facilitate the escape from custody of a person who is under lawful detention.

12.8 The Australian Privacy Act's National Privacy Principle (NPP) 6 also contains specific exceptions to access, including where providing access would be likely to prejudice:[984]

- an investigation of possible unlawful activity;
- the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
- the enforcement of laws relating to the confiscation of proceeds of crime;
- the protection of the public revenue;
- the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
- the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body.

12.9 The Australian Freedom of Information Act allows access to information to be denied where disclosure would:[985]

- prejudice the conduct of an investigation or the enforcement or proper administration of the law in a particular instance;
- disclose the existence or identity of a confidential source of information in relation to the enforcement or administration of the law;
- disclose lawful methods for dealing with breaches or evasions of the law that would, or would be reasonably likely to, prejudice the effectiveness of those methods; or
- prejudice the maintenance or enforcement of lawful methods for the protection of public safety.

984 Privacy Act 1988 (Cth), sch 3, NPP 6.1(i) and (j).

985 Freedom of Information Act 1982 (Cth), s 37. See also Archives Act 1983 (Cth), s 33(1)(f)(ii).

Law reform options

12.10 In an earlier review of the New Zealand Privacy Act, the Privacy Commissioner recommended that consideration be given to redrafting the "maintenance of the law" withholding ground for access requests to make more plain the constituent law enforcement interests protected, noting that the British Columbia provision is more easily understandable on its face, whereas the meaning of the New Zealand provision only becomes apparent from the case law (including OPC case notes).[986] The Privacy Commissioner suggested that section 27(1)(c) be rewritten so that it may be clearly understood by all those involved, including:[987]

- staff in law enforcement agencies;
- requesters; and
- bodies exercising review functions.

However, the Privacy Commissioner noted that most "maintenance of law" agencies have a good understanding of the withholding ground.[988]

12.11 We agree that further development of section 27(1)(c) may provide greater clarity to law enforcement agencies about the parameters of the law enforcement access exception. Issues for further consideration include the specific grounds for refusing access and whether a revised maintenance of the law exception should be expressly linked to the functions of law enforcement agencies (like, for example, the Australian Privacy Act's NPP 6.1(j)) or whether it should apply more broadly (as per the current provision).[989]

12.12 In terms of identifying the particular law enforcement interests that should be targeted by the maintenance of law exception, some guidance may be provided by clause 55(3) of the Search and Surveillance Bill 2009 (albeit in a different context), which provides that before a judge may order notification to a target of law enforcement surveillance (where a surveillance device warrant was improperly issued or has been breached) the public interest in such notification must outweigh any potential prejudice to the following law enforcement interests:

- any investigation by the law enforcement agency;
- the safety of informants or undercover officers;
- the supply of information to the law enforcement agency; and
- any international relationships of the law enforcement agency.

---

986 *Necessary and Desirable* para 4.2.17; recommendation 48.

987 *Necessary and Desirable* para 4.2.18. The Privacy Commissioner further noted that any change would need to be made in parallel with changes to equivalent provisions in the Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987: para 4.2.19.

988 *Necessary and Desirable* para 4.2.19.

989 On this point, see Office of the Privacy Commissioner *Law Enforcement Information and Related Issues: Review of the Privacy Act 1993 Discussion Paper 8* (Wellington, 1997) 9, which notes that the maintenance of law exception for the purposes of the access principle differs in some respects from the maintenance of law exception to principles 2, 3, 10 and 11.

12.13 We note that any reform to the section 27(1)(c) withholding ground would need to be part of a generic reform that also encompassed the equivalent provisions in the official information statutes[990] and criminal disclosure legislation,[991] in order to maintain consistency.

Q144 Should section 27(1)(c) include more specific law enforcement grounds for the withholding of personal information about a requester? If so, which specific grounds should be included?

12.14 The website of the New Zealand Privacy Commissioner already provides some information on the "maintenance of law" ground,[992] but it could be helpful for law enforcement agencies and others if the Privacy Commissioner provided more detailed guidance about the operation of that ground.[993]

Q145 Would it be helpful if the Privacy Commissioner provided information or commentary about the law enforcement grounds for refusing access?

Criminal disclosure and requests from prisoners

12.15 Before 29 June 2009 defendants in criminal proceedings often relied on the Privacy Act to obtain from the Police information held about them relevant to the offence with which they were charged. On that date, however, the Criminal Disclosure Act 2008 came into force. It provides for initial disclosure, full disclosure and additional disclosure by providing a wide range of information held by the prosecution relevant to the proceedings, including witness statements, lists of exhibits, and copies of information supplied to the prosecution.[994] There is a wide range of withholding grounds, including prejudice to maintenance of the law, that disclosure would be likely to facilitate the commission of another offence, and that the information has previously been made available to the defendant.[995]

12.16 This disclosure regime under the Criminal Disclosure Act is a continuing obligation on the prosecution, applicable before and during a trial, and pending appeal. The defendant's entitlement to full disclosure under the Act ceases on the expiry of the time for lodging an appeal against conviction.[996] An amendment to the Privacy Act in 2009 provides that an agency may refuse to provide information to a defendant under principle 6 if the information could be sought

990 Official Information Act 1982, ss 27(1)(a) and 6(c); Local Government Official Information and Meetings Act 1987, ss 26(1)(a) and 6(a).

991 Criminal Disclosure Act 2008, s 16(1)(a).

992 Office of the Privacy Commissioner "Maintaining the Law" www.privacy.org.nz/maintaining-the-law (accessed 5 February 2010).

993 Compare the guidance provided by the Australian Privacy Commissioner: *Information Sheet on Unlawful Activity and Law Enforcement* (Sydney, 2001).

994 Criminal Disclosure Act 2008, ss 12–14.

995 Criminal Disclosure Act 2008, s 16.

996 Criminal Disclosure Act 2008, s 13(6).

under the Criminal Disclosure Act, or if the information has in fact been disclosed to or withheld from the defendant under that Act.[997] To that extent, then, the Criminal Disclosure Act overrides the Privacy Act.

12.17 A section of the Privacy Act, section 31, used to provide that access could be denied to any person who had been imprisoned to information relating to the offence of which the person had been convicted. However, that section never came into force, and was repealed in 2009.[998]

12.18 It used to be a concern under the regime before the Criminal Disclosure Act that prisoners might obtain under the Privacy Act certain types of information – for example information about sexual or violent offences – which would then be circulated among prisoners and acquire cachet. There might also be other types of conduct – for example, publication on the internet – which could cause distress to families and others.

12.19 The question is whether, since the coming into force of the Criminal Disclosure Act, there might be information not covered by that Act which could be requested under the Privacy Act with similar undesirable consequences. If so, there might be a case for reviving section 31. But in the meantime we suggest that it is probably best to monitor the operation of the Criminal Disclosure Act and see if any problems of the kind to which we have adverted arise.

Q146 We believe that, as a result of the coming into force of the Criminal Disclosure Act 2008 and section 29(1)(ia) of the Privacy Act 1993, there is presently no need to make provision for limiting access by prisoners to information. Do you agree?

Volume of access requests

12.20 The number of access requests to law enforcement agencies such as the Police is high. Coupled with requests under other enactments this can impose a substantial burden on them. The amount of material to be reviewed for some access requests also has an impact on police resources. According to the Police, over 40,000 Official Information, Privacy Act and Criminal Disclosure requests are issued each year. There is some frustration with repeat requests that tie up police time and resources.

12.21 In an earlier report,[999] the Law Commission recommended that agencies should be able to refuse repeat requests under the OIA, provided no reasonable grounds exist for that person to request the information again. This recommendation was not implemented. But such a provision does appear now in the Criminal Disclosure Act 2008.[1000] In chapter 4 we dealt generally with the question of

997 Privacy Act 1993, s 29(1)(ia), added by the Criminal Disclosure Act 2008, s 39(1).

998 Criminal Disclosure Act 2008, s 39(2).

999 New Zealand Law Commission *Review of the Official Information Act 1982* (NZLC R40, Wellington, 1997) 7, E23.

1000 Criminal Disclosure Act 2008, s 16(1)(m): information to which the defendant would otherwise be entitled may be withheld if "the information has previously been made available to the defendant".

repeat requests, and favoured a solution of the kind earlier recommended by the Law Commission. The "frivolous or vexatious" ground[1001] as a means of weeding out repeat requests is also discussed in chapter 4.

INFORMATION SHARING

12.22 In this section we outline:

- issues that arise where individuals, private agencies and public agencies provide personal information about individuals to law enforcement agencies;
- the mechanism in Schedule 5 of the Privacy Act that allows justice sector and other agencies to exchange particular items of personal information for certain purposes; and
- issues that arise where law enforcement agencies wish to share personal information with each other or with overseas law enforcement agencies.

12.23 Information sharing between public sector agencies is discussed in chapter 10. In particular, that chapter considers issues raised by inter-agency initiatives involving a range of public agencies, including the Police.

Information sharing with law enforcement agencies under principle 11

Maintenance of law exception to principle 11

12.24 Principle 11 allows a third party to disclose personal information to a law enforcement agency where the third party believes on reasonable grounds that disclosure is necessary for the maintenance of the law by the law enforcement agency, including, more specifically, the prevention, detection, investigation, prosecution, and punishment of any offences.[1002] This allows agencies to:

- "volunteer" or report information to law enforcement agencies, where it may be in their interests to do so (such as where there is criminal offending against the third party agency) or in the interests of their clients or customers (such as in the case of reporting identity theft); and
- respond to requests for information from law enforcement agencies.

12.25 Disclosure by an agency under principle 11 in response to a request from a law enforcement agency is discretionary, rather than mandatory. Even where the agency believes on reasonable grounds that disclosure may be necessary to avoid prejudice to the maintenance of law, it cannot be compelled to disclose personal information to a law enforcement agency in the absence of a warrant or other judicial order (such as a production order). We note that the discretionary nature of disclosure under the Privacy Act is made explicit in a note to the Australian Privacy Act:[1003]

> Nothing in sub-clause 2 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

1001 Privacy Act 1993, s 29(1)(j).

1002 Privacy Act 1993, s 6, principle 11(e)(i).

1003 Privacy Act 1988 (Cth), sch 3, NPP2, note 2.

12.26 It may be that some agencies take an overly cautious approach to disclosing information in response to police requests, even when the "maintenance of law" exception applies. However, any attempt to limit the discretionary nature of principle 11 would give rise to concerns that law enforcement agencies could require disclosure from third party agencies outside the oversight of the warrant regime. This would be contrary to fundamental principle. Nevertheless, we think that the maintenance of law exception is not particularly "user-friendly" and could be clarified to make it clearer for agencies to assess whether disclosure for law enforcement purposes is permitted under principle 11.

Options for reform of the maintenance of law exception

12.27 As in the case of access requests, discussed above, we wonder whether it might be possible to define the "maintenance of law" exception to principle 11 in more detail. We have considered formulations from other jurisdictions. For example, the Canadian Personal Information Protection and Electronic Documents Act permits disclosure where disclosure is:

- required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;[1004]
- made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that:[1005]
  - it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
  - the disclosure is requested for the purposes of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
  - the disclosure is requested for the purpose of administering any law of Canada or a province;
- made on the initiative of the organisation to an investigative body, a government institution or a part of a government institution and the organisation:[1006]
  - has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
  - suspects that the information relates to national security, the defence of Canada or the conduct of international affairs; or
- made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.[1007]

1004 Personal Information Protection and Electronic Documents Act SC 2000, s 7(3)(c).

1005 Personal Information Protection and Electronic Documents Act SC 2000, s 7(3)(c.1).

1006 Personal Information Protection and Electronic Documents Act SC 2000, s 7(3)(d).

1007 Personal Information Protection and Electronic Documents Act SC 2000, s 7(3)(h.2).

12.28 The Australian Privacy Act includes notes to some National Privacy Principles:

- Note 1 to NPP2 (use and disclosure) states that the principle "is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions."
- Note 3 to NPP2 requires an organisation that uses or discloses personal information under this ground to make a written note of the use or disclosure.

12.29 We think that consideration should be given to redrafting the maintenance of law exception to provide additional clarity, drawing on the overseas formulations. We note that certainty, simplicity and clarity are important values and goals in the context of law enforcement[1008] and these goals would be served by reviewing the maintenance of law exception to ensure it is fit for purpose.

Q147 We suggest that the maintenance of the law exception should be redrafted for greater clarity. Do you agree?

12.30 We note that some formulations of the maintenance of law exception use a separate exception for disclosure by an agency to report suspected offending. For example, NPP 2 of the Australian Privacy Act contains a separate exception to the use and disclosure principle that applies where:[1009]

> the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

12.31 The Canadian Personal Information Protection and Electronic Documents Act also has a separate exception for disclosure on the initiative of the information holder agency, in the absence of a law enforcement request.[1010]

12.32 The option of distinguishing between disclosure by law enforcement agencies and disclosure by other agencies for law enforcement purposes was raised by the Privacy Commissioner in an earlier review.[1011] It was suggested that there could be separate maintenance of law exceptions for disclosure by:

- a law enforcement agency in the exercise of its functions; and
- another agency to a law enforcement agency where there are reasonable grounds to believe that disclosure is necessary to assist the law enforcement agency in the exercise of its functions in relation to an offence.

1008 See discussion of the law enforcement values of effectiveness, simplicity, certainty, responsiveness and human rights consistency in the context of law enforcement search and seizure powers in New Zealand Law Commission *Search and Surveillance Powers* (NZLC R97, Wellington, 2007) chapter 2.

1009 Privacy Act 1988 (Cth), sch 3, NPP 2.1(f). The ALRC supports this exception: see Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 25.97 and 25.189.

1010 Personal Information Protection and Electronic Documents Act SC 2000, s 7(3)(d).

1011 Office of the Privacy Commissioner *Law Enforcement Information and Related Issues: Review of the Privacy Act 1993 Discussion Paper* (Wellington, 1997) 7–8. However, this suggestion was not taken forward due to lack of submissions in support.

Separate exceptions may help to clarify the grounds on which agencies can exercise the discretion to disclose personal information for law enforcement purposes. We invite comment on whether separate maintenance of law exceptions would help to add clarity.

> Q148 Should there be separate maintenance of the law exceptions for the disclosure of personal information (i) to a law enforcement agency upon request, (ii) to a law enforcement agency in the absence of a request, and (iii) by a law enforcement agency?

12.33 We have noted that the Australian Privacy Commissioner has published an Information Sheet that provides commentary on the law enforcement exception to the use and disclosure principle.[1012] We raise for consideration whether information or commentary from the New Zealand Privacy Commissioner may help to provide further clarity about the operation of the maintenance of law exception to the use and disclosure principles.[1013]

> Q149 Would it be helpful if the Privacy Commissioner provided information or commentary about the maintenance of the law exception to the use and disclosure principles?

Section 21 of the Bill of Rights Act 1990

12.34 Although it is only peripherally relevant to our review of the Privacy Act, we have considered the potential impact of section 21 of the Bill of Rights Act 1990 where people and agencies disclose personal information to law enforcement agencies in response to a request for that information. Section 21 provides:

> Everyone has the right to be secure against unreasonable search and seizure, whether of the person, property, or correspondence or otherwise.

Under section 21, law enforcement actions that intrude on reasonable expectations of privacy can be reviewed by the courts to assess whether, on balance, such actions are unreasonable.[1014] Most cases to date have dealt with physical intrusions into privacy such as searches of the person or property. There is a question as to how far section 21 is relevant to encroachments on informational privacy in the absence of a physical intrusion.

12.35 One view is that section 21 regulates the exercise of coercive powers, rather than voluntary disclosures of information from third parties.[1015] Disclosures of information responding to warrantless requests for information can be considered "voluntary" as there is no exercise of a coercive law enforcement power given that the agency holding the information can decline the request.

1012 Australian Privacy Commissioner *Information Sheet on Unlawful Activity and Law Enforcement* (Sydney, 2001).

1013 Compare Q145 above.

1014 See New Zealand Law Commission *Privacy: Concepts and Issues (*NZLC SP19, Wellington, 2008) paras 4.98–4.104.

1015 See Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (LexisNexis, Wellington, 2005) para 18.11.5.

12.36 However, New Zealand case law confirms that the provision of information in response to a police request may be a search for purposes of section 21 where the informant can be regarded as acting as an agent of the police. In *R v H,*[1016] the Court of Appeal stated:[1017]

> Wholly private conduct is left to be controlled by the general law of the land. Thus the Bill of Rights does not extend to any search or seizure undertaken privately by a private individual. But if there is governmental involvement in a search or seizure actually carried out by an informer or other private individual, that may attract the Bill of Rights' protections.
>
> In some cases the dividing line between governmental action and purely private action may be hard to draw. However, if a police officer or other official participates in or instigates a search and seizure the objects of the Bill of Rights would be frustrated if that officer's conduct was not subject to s 21.

The court found that documents initially supplied to the police by an accountant that were evidence of corruption by his employer were volunteered by the accountant and were the product of a private search and seizure (and therefore outside the ambit of the section 21 review). Subsequently, the police solicited further information from the accountant. The court found that in relation to this further information, the accountant was effectively acting as the agent of the government and the search should be treated as governmental in character.[1018] Further, the search was found to be unreasonable in terms of section 21.

12.37 *R v H* was distinguished in *R v Cox*,[1019] a case involving co-operation between Vodafone and the police in targeting the text messages of certain suspects. In that case, the Court of Appeal found that the voluntary supply of text messages by Vodafone "as a good corporate citizen" was beyond reproach, although it noted that there was sufficient police involvement and instigation to engage section 21 if the police's actions were unreasonable.[1020] Nevertheless, the actions of the police were not unreasonable, in part due to the court's conclusion that the call data and search warrant processes were not particularly well-suited to obtaining texting information, and also because the court regarded the information as "belonging" to Vodafone.[1021] The Court of Appeal declined to give weight to the appellant's privacy interest.[1022]

1016 *R v H* [1994] 2 NZLR 143 (CA).

1017 *R v H* [1994] 2 NZLR 143, 147 (CA). See also *R v Grayson and Taylor* [1997] 1 NZLR 399, 407 (CA), noting the decision in *R v H* and confirming that a search and seizure carried out by a private individual will be governmental in character and subject to the Bill of Rights protections if there is governmental instigation or involvement in the search.

1018 A noteworthy feature of the case was that the police refrained for 20 months from obtaining and executing a search warrant after they reasonably could have done so. See *R v Cox* (2004) 21 CRNZ 1, para 60 (CA).

1019 *R v Cox* (2004) 21 CRNZ 1, Anderson P, McGrath and William Young JJ, paras 68 and 69 (CA).

1020 *R v Cox* (2004) 21 CRNZ 1, para 38 (CA).

1021 *R v Cox* (2004) 21 CRNZ 1, paras 59, 66 and 69 (CA).

1022 *R v Cox* (2004) 21 CRNZ 1, para 69 (CA). Compare *R v Zutt* (2001) 19 CRNZ 154, 157, Tipping, McGrath and Heron JJ (adopting the findings of the High Court Judge). See also *R v Beattie* (31 May 2005) HC AK CR1 2003-004-25599, CIV 2004-404-6797, Allan J; *S v Police* (2002) 22 FRNZ 28 Panckhurst J (HC); *R v Ellerington* (13 November 2007) HC WN CR1 2006-032-3536 Clifford J; and, in Canada, *R v Dyment* [1988] 2 SCR 417; *R v Plant* [1993] 2 SCR 28; *R v Gomboc* [2009] AJ No 892; *R v Lillico* (1994) 92 CCC (3d) 90; *R v Weir* [2001] AJ No 869.

12.38 Law enforcement agencies will need to consider the application of section 21 of the Bill of Rights Act in weighing up whether to obtain personal information by way of a request to a party that holds that information. A relevant consideration is likely to be whether the law enforcement agency is effectively attempting to circumvent the need to apply for a warrant. For the purposes of this issues paper we need take the matter no further.

Information sharing with law enforcement agencies under the Official Information Act

12.39 In chapter 11, we discuss the issue of whether or not requests under the Official Information Act can be made between public agencies (including law enforcement agencies) as a means of exchanging personal information.

Information sharing under Part 11 and Schedule 5

12.40 Part 11 of the Privacy Act creates a mechanism that allows certain law enforcement information that is specified in Schedule 5[1023] to be accessed by particular public agencies in accordance with the authorisation provided by Schedule 5. A Schedule 5 authorisation overrides the information-sharing requirements of the privacy principles that would otherwise apply, such as obtaining the prior consent of the person the information relates to. Access to some Schedule 5 information is only limited by agency, while access to other Schedule 5 information is limited both by agency and by the purpose for which the agency may access the information.[1024]

12.41 This specific mechanism for the sharing of law enforcement information between public agencies is unique to New Zealand and has no direct equivalent in other comparable jurisdictions.[1025] It has its origins in the Wanganui Computer, a centralised database of law enforcement information to which various agencies had access under the Wanganui Computer Centre Act 1976. This Act was subsequently replaced by the Privacy Act, with the mechanism for justice sector

1023 Records specified in Schedule 5 include records of the **Ministry of Justice** relating to court processing, details of hearings, enforcement of fines and other orders, suspended sentences, and non-performance of bail conditions; **Police** records relating to details of overseas hearings, police temporary index file, offender identity, victim identity, medical details, traffic offences, vehicles of interest, wanted persons, missing persons, firearms licences, protection orders and restraining orders; **Land Transport** records relating to the driver licence register, the transport services licensing register, demerit points, the rail licensing register; **Ministry of Transport** records relating to the motor vehicles register and road user charges; **Department of Correction** records relating to community-based sentences and records of inmates. See also Ministry of Justice *Justice Information Stocktake: What's Where, Information Held and Used By the Justice Sector* (Wellington, 2007) for an overview of information sharing within the criminal justice sector.

1024 See *Necessary and Desirable* para 11.1.23.

1025 While the Schedule 5 mechanism is unique, bulk access to law enforcement information also occurs in other jurisdictions under other mechanisms. For example, in the United Kingdom, the Police Act 1997 is a statutory regime that provides for the National Criminal Intelligence Service to provide criminal intelligence to police forces and to other law enforcement agencies (including government departments). The Police National Computer is accessible by criminal justice agencies and all UK police forces. A linked system, the Violent and Sexual Offenders Register or ViSOR, is used jointly by police, probation and prison staff under Multi-Agency Public Protection Arrangements: Joseph Rowntree Reform Trust Ltd. *Database State* (London, 2009) 23. See also chapter 10 for discussion of information-sharing in overseas jurisdictions.

law enforcement information-sharing being carried over into Schedule 5.[1026] The mechanism was established in order to facilitate the bulk access to personal information necessary for the functioning and operation of the justice sector. The Schedule 5 mechanism was considered a necessary alternative to the privacy principles disclosure mechanism, which otherwise requires a case-by-case assessment of whether disclosure for the purpose of information-sharing is permitted.[1027] The advantage of the Schedule 5 approach is that it provides a degree of certainty and clarity for agencies that the sharing of particular law enforcement information is not in breach of the privacy principles.

12.42 However, one perceived problem is that some Schedule 5 agencies tend to rely solely on Schedule 5 for information-sharing, to the exclusion of other authorised means, for example, case-by-case information sharing permitted under principle 11. This can frustrate the functions of other agencies if Schedule 5 does not apply to the information-sharing requested. Other difficulties with Schedule 5 include the fact that it is prescriptive rather than flexible. Agencies find that it does not always reflect actual information-sharing practices and authorisations can be incomplete or become outdated. Amending Schedule 5 requires legislative amendment, a more onerous and time-intensive procedure than the Order in Council process that applied up until 1 July 1997. We note from the legislative history that Schedule 5 is frequently amended as a consequence of departmental restructuring and legislative activity that affects the Schedule 5 agencies or the law enforcement information that is subject to access under Schedule 5.

12.43 Currently, where new agencies wish to be included in Schedule 5 or where Schedule 5 agencies require expanded access to law enforcement information, changes to Schedule 5 can be promoted within a variety of legislation.[1028] The Ministry of Justice is concerned that the current legislative approach to amending Schedule 5 carries the risk that the integrity of Schedule 5 may be undermined and suggests that a "gatekeeper" agency should co-ordinate legislative changes in accordance with certain criteria. In the meantime, the Ministry of Justice has developed a questionnaire for agencies wishing to gain access to law enforcement information under Schedule 5.[1029] According to the Ministry, a full baseline review of Schedule 5 is needed, which looks at what law enforcement information each agency needs and why. [1030]

12.44 Another issue is whether there are adequate checks and balances in place in relation to Schedule 5 information sharing. Once information sharing has been authorised by Schedule 5, there are no further restrictions or accountability provisions relating to the sharing. This can be contrasted with the accountability requirements for information matching under Part 10, which include a written

1026 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington) LEF1.5 (last updated 2007); *Necessary and Desirable* paras 11.1.1, 11.1.14 and 11.1.24.

1027 See *Necessary and Desirable* para 11.1.22.

1028 See, for example, Land Transport Amendment Act 2009, sch 2 (amending the Privacy Act 1993, sch 5).

1029 Justice Sector Information Strategy Group, Ministry of Justice *Law Enforcement Information Sharing Under the Privacy Act 1993: Principles For Assessing Whether An Agency Should Be Included in Schedule 5*. This asks agencies to identify the information sought, where it is held, the purpose for accessing the information, steps to be taken to protect the information from other uses, frequency and volumes of access, whether the agency currently access the information, and whether the agency has information matching agreements with the relevant agency.

1030 Meeting between the Law Commission and the Ministry of Justice, 30 March 2009.

agreement between the two specified agencies reflecting the information matching rules (with a copy required to be sent to the Privacy Commissioner), regular reporting by specified agencies to the Privacy Commissioner, and regular review by the Privacy Commissioner.[1031]

Law reform options

12.45 In an earlier review, the Privacy Commissioner concluded that Part 11 and schedule 5 fulfil a valuable function and provide a degree of transparency.[1032] More recently, the Office of the Privacy Commissioner has reported that agencies find the Schedule 5 mechanism less than transparent and difficult to update in a timely manner.[1033] In consultation with a group of Privacy Act experts,[1034] there was a divergence of views about the Schedule 5 mechanism, with one participant thinking Schedule 5 represents an archaic approach, while other participants felt that it has some uses, such as providing some parameters around law enforcement information sharing, providing some indication to the public of the information sharing that takes place, and, in some cases, articulating the purposes of such information sharing.

12.46 The Office of the Privacy Commissioner has identified the following specific options:[1035]

- retain Schedule 5 as a specific law enforcement information sharing mechanism in legislation, given particular sensitivities over law enforcement information sharing, and the history of the Wanganui Computer;
- replace Schedule 5 with equivalent regulations to "declutter" the Privacy Act;[1036] and
- provide for law enforcement information-sharing in a code of practice.[1037]

12.47 Whichever form the mechanism takes, there is also the option of building in additional transparency and accountability measures. In our view, bulk accessing of law enforcement information between public agencies has some similar attributes to data matching, and we raise for consideration whether some of the measures specified in Part 10 could also be of value in the context of Schedule 5 information sharing. Like information matching, we think that law enforcement information sharing should be:[1038]

- subject to rules developed by the Privacy Commissioner;
- undertaken pursuant to an agreement between the agencies involved, with a copy of the agreement being provided to the Privacy Commissioner;

1031 These accountability requirements are discussed in chapter 9 above.

1032 *Necessary and Desirable* para 11.3.6.

1033 Office of the Privacy Commissioner to the Law Commission (10 November 2008) Email.

1034 Privacy Experts Forum held at the Law Commission on 8 May 2008.

1035 Office of the Privacy Commissioner "Briefing for the Law Commission on Privacy Act 1993, Part 11, Law Enforcement Information" (5 March 2009).

1036 This was considered by the Privacy Commissioner in *Necessary and Desirable* para 11.5.7. However, at that time, the Commissioner's preference was to reactivate the Order in Council process for amending Schedule 5.

1037 This could build on the Justice Sector Unique Identifier Code 1998.

1038 Unlike information matching, the requirement for notice of adverse action and limits on taking adverse action against an individual would not be included.

- reported to the Privacy Commissioner on a regular basis; and
- reported on by the Privacy Commissioner in her annual report.

12.48 An alternative to these specific reform options would be for one of the generic information-sharing options outlined in chapter 10 to apply to law enforcement information sharing as a type of public sector information sharing. If a generic mechanism for public sector information sharing is adopted, the need for a specific mechanism for law enforcement information sharing may be removed, unless there are particular issues relating to law enforcement information sharing that continue to require a specific response. However, if the development of a generic public sector information-sharing mechanism is predicated on information sharing for benign or beneficial purposes, law enforcement information sharing would continue to require its own mechanism.

Q150 Should Schedule 5 law enforcement information sharing continue to be dealt with in a specific Schedule to the Privacy Act? Alternatively, should this be dealt with in specific regulations, or in a specific code of practice?

Q151 Should additional transparency and accountability measures (like those that apply to information matching) also be applied to law enforcement information sharing? Alternatively, could Schedule 5 law enforcement information sharing be dealt with adequately under one or more of the generic information-sharing options outlined in chapter 10?

12.49 If Schedule 5 is retained in some form, we think that two issues should be addressed. The first relates to whether local authorities should be authorised to have access to law enforcement information under Schedule 5. Section 112 provides that local authorities may be authorised to access law enforcement information under Schedule 5 by Ministerial notice in the Gazette where Schedule 5 permits that. It currently does so in the case of the driver licence register and the motor vehicles register. In an earlier review,[1039] the Privacy Commissioner found that local authority access to law enforcement under this section was unnecessary and thought that section 112 should probably be deleted.[1040] It may be more appropriate to deal with local authority access to the two specified registers under the public register provisions of the Privacy Act,[1041] or in the specific legislation setting up the registers,[1042] rather than under Schedule 5.

Q152 Is there any reason for Part 11 and Schedule 5 to continue to provide for local authorities to have access to any law enforcement information?

1039 *Necessary and Desirable* paras 11.4.6–11.4.7.

1040 *Necessary and Desirable* recommendation 139.

1041 Privacy Act 1993, Part 7.

1042 The Law Commission has conditionally recommended the repeal of the public register provisions of the Privacy Act: *Public Registers* (NZLC R101, Wellington, 2008) para 5.94.

12.50 The second issue is whether the power to amend Schedule 5 by Order in Council[1043] should be reinstated. In an earlier review, the Privacy Commissioner recommended that the power should be reinstated subject to a five year sunset clause.[1044] We agree that the process of legislative amendment to Schedule 5 is lengthy and cumbersome and that a power to amend the Schedule by Order in Council would be more flexible. We note, however, that it would be important to ensure that any such process should be accompanied by proper controls.

12.51 The reinstatement of the Order in Council process under section 113 would permit the Minister of Justice, after consultation with the Privacy Commissioner, to advise the Governor-General to make an amending Order. This would make the Ministry of Justice the responsible agency for considering agency requests for changes to Schedule 5 and explicitly allow for input from the Privacy Commissioner. The Ministry of Justice could then develop appropriate processes and criteria for assessing agency requests for changes to Schedule 5. The Minister would need to be satisfied that the public interest in authorising the information sharing outweighs adherence to the privacy principles, and agencies proposing new information sharing initiatives might be required to undertake a privacy impact assessment.

12.52 Orders would be subject to disallowance. However, there is a case for retaining Parliamentary scrutiny over significant new information-sharing initiatives.[1045] One option might be to give the Privacy Commissioner a stronger consultation right that includes an effective power to "veto" the Order in Council process where any proposed amendment represents a significant, new or expanded information-sharing initiative. In such a case, the Schedule 5 amendment would be subjected to the full legislative process.

12.53 We do not think that it would be necessary to make the Order in Council power subject to a sunset clause. Section 114 of the Privacy Act, the original sunset clause, was included to allow for changes to Schedule 5 as agencies migrated off the Wanganui Computer. However, the legislative history of Schedule 5 shows numerous changes for other reasons such as departmental restructurings and other legislative initiatives and we anticipate that Schedule 5 will likely continue to be subject to regular amendment.

Q153 Should the power to amend Schedule 5 by Order in Council be reinstated? Should the power be subject to a sunset clause? What safeguards should be built into the process?

1043 Privacy Act 1993, s 113 (expired).

1044 *Necessary and Desirable* recommendation 142.

1045 See Alan Travis "Tories outline plans to shrink 'surveillance state'" (16 September 2009) *The Guardian* London www.guardian.co.uk (accessed 17 September 2009).

Information sharing between New Zealand law enforcement agencies

12.54 Outside bulk information sharing under Schedule 5, whether law enforcement agencies such as the Police (including the Organised & Financial Crime Agency), the Serious Fraud Office, Customs and other departments with enforcement units such as the Ministry of Fisheries and the Department of Internal Affairs, can share information with each other (for example referring information to another agency for enforcement purposes) depends on the operation of the purpose principle (principle 1) and the maintenance of law exceptions to the use and disclosure principles.

12.55 The threshold question under principle 1 is whether the collection of personal information is for a lawful purpose connected with a function or activity of the law enforcement agency. The functions of the police are set out in the Policing Act 2008 and include:[1046]

- keeping the peace;
- maintaining public safety;
- law enforcement; and
- crime prevention.

These broadly stated purposes should generally allow the police to collect personal information relating to suspected criminal offending. Sharing that information with another law enforcement agency should generally be permitted under the first exception (disclosure is for one of the purposes in connection with which the information was obtained, or for a directly related purpose)[1047] or under the maintenance of law exception.[1048]

Reform options

12.56 One option would be to redraft the maintenance of law exception, as discussed above, to clarify the sharing of personal information between law enforcement agencies for law enforcement purposes.

12.57 Other options raised in chapter 10 may be worth considering in this context, such as guidelines or a code of practice. In the event that a broader framework replaces the current form of Schedule 5, another option might be to accommodate such information sharing within that framework.

Q154 Should the maintenance of the law exception to the disclosure principle be redrafted to clarify that personal information may be shared between law enforcement agencies for law enforcement purposes? Should any other mechanism to facilitate information sharing between law enforcement agencies be considered?

1046 Policing Act 2008, s 9.

1047 Privacy Act 1993, s 6, principle 11 (a).

1048 Privacy Act 1993, s 6, principle 11 (e)(i).

Information sharing between New Zealand law enforcement agencies and law enforcement agencies in other jurisdictions

12.58 In an earlier review, the Privacy Commissioner considered whether any provision was needed to allow New Zealand law enforcement agencies to share personal information with their counterparts overseas.[1049] While the Privacy Commissioner concluded that the maintenance of law exception to the disclosure principle is not broad enough to cover offshore disclosures by law enforcement agencies, the Privacy Commissioner did not recommend any change on the basis that he had no evidence that this created any real problem for law enforcement agencies.

12.59 In response to this review, we have heard from the Police that they have had difficulties responding to requests for assistance from overseas law enforcement agencies as they cannot rely on the maintenance of law exception to the disclosure principle, and the regime established by the Mutual Assistance in Criminal Matters Act 1992 does not apply if an investigation has not actually commenced.

12.60 One option might be to amend the maintenance of law exception to encompass disclosures to offshore law enforcement agencies; however, there are also other options, such as amending the Mutual Assistance in Criminal Matters Act or basing such disclosures on the model in section 281 of the Customs Act 1996. The Customs Act model would allow a New Zealand law enforcement agency to disclose specified information to law enforcement overseas agencies on certain conditions, including a prior written agreement between the New Zealand and overseas agencies that requires prior consultation with the Privacy Commissioner and certain other requirements.

12.61 Another model that might be used is that contained in the Social Welfare (Transitional Provisions) Act 1990.[1050] This provides for mutual assistance provisions in reciprocity agreements with other countries in relation to social security benefits.[1051] Section 19C sets the terms and conditions for information sharing.

12.62 The Ministry of Justice is currently working on an information sharing arrangement between Australia and New Zealand to allow the respective immigration authorities to share criminal history information. The model resulting from this work may also be a useful point of comparison.

12.63 We also discuss cross-border information sharing in chapter 10, and ask a question how legal provision for such information sharing should be made.

Information sharing with non-law enforcement agencies

12.64 Law enforcement agencies also participate in information sharing with other public sector agencies and non-governmental organisations under inter-agency initiatives. The issues that arise in relation to this form of information sharing are discussed in chapter 10.

1049 *Necessary and Desirable* paras 2.13.6 – 2.3.10.

1050 See discussion in chapter 9.

1051 Social Welfare (Transitional Provisions) Act 1990, ss 19 and 19A.

Chapter 13
Technology

13.1 In this chapter we outline some key technological developments and consider the Privacy Act issues that they may give rise to. The range of topics covered is necessarily selective, and it is by no means a comprehensive survey.[1052] The pace of change in this area means that new technological issues are constantly arising. We have selected topics that affect large numbers of New Zealanders or give rise to important privacy issues. At the end of the chapter we ask for views as to whether there are any other technology issues that submitters believe warrant particular consideration. We are not technology experts, and we invite comments and submissions from those who are. We also welcome the views of anyone with an interest in these topics.

13.2 We have endeavoured to ensure that the material in this chapter is up-to-date at the time of writing. Due to the rapid pace of change, however, some of the statements made, and material referred to in this paper, may quickly become outdated.

BACKGROUND

13.3 Technological advances have made it technically and economically feasible to collect, use, store and re-use massive amounts of personal information in a variety of contexts for multiple purposes. These developments have been embraced in both the public and private sectors, where there is significant reliance on the collection, use, sharing and repackaging of personal data. Consequently, personal data has become increasingly commoditised:[1053]

> The provision of public services of all kinds has become dependent on data collection, sharing, and other related practices. Government activity is dependent on the use of personal data. The economy is fuelled by information processing. Many companies build their businesses around the collection and analysis of data.

13.4 The information practices which these technological developments give rise to are on a new scale from traditional paper records or early computer databases. The Office of the Privacy Commissioner's current Statement of Intent notes that rapidly changing technologies, internet fraud and safety, cloud computing and

1052 See also Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) chapter 9.

1053 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009) para 47.

cross-border data processing all raise challenging information and privacy issues.[1054] The impacts of the internet and social networking on privacy, in particular young people's privacy, are increasingly important:[1055]

> Opinion surveys indicate that New Zealanders are concerned about the misuse of personal information and invasion of individual privacy by technology. Unease exists around privacy intrusions in areas such as social networking, the internet, employment, finance, telecommunications and health.

13.5 The digital revolution continues to create a wealth of personal data about people and their activities. Some might ask whether there is any realistic prospect that personal privacy can be protected in the new digital era, and whether it is worth attempting to protect digital privacy, given the economic benefits to the private sector and the increased efficiency to the public sector that technological developments relating to data have given rise to.

13.6 Nevertheless, while technological transformations undoubtedly bring great benefits and efficiencies, they also create potentially significant societal and individual costs,[1056] such as loss of control over the collection and use of personal information, the potential for increased surveillance and an associated chilling effect on citizens, reduced trust in relationships between citizens and business or government with consequential reduced participation, and an increased risk of detrimental consequences including identity crime.[1057] There are also commercial benefits to privacy protection (whether online or offline) including customer retention, reduced reputational risk and efficiency gains. We therefore see data protection as continuing to have an important role in the digital context.

13.7 In fact, the role of data protection may become even more crucial in light of technological developments. As people engage more completely with digital technologies, the amount of digital data proliferates, as do the number of spin-off profiles that begin to accrue:[1058]

> [T]he danger is that what is relevant is no longer personhood – the recognition of a person as having status as a person – but rather a profile – the recognition of a pattern of past behaviour. … The ability to control the use of one's identity information is crucial for reminding others that there is a person behind data and enabling that person to have full status when dealing with others.

1054 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 3.

1055 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 10.

1056 See discussion of Solove's harm-based analysis in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 3.26–3.32.

1057 See discussion of informational privacy risks in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 3.40–3.49.

1058 OECD Directorate for Science, Technology and Industry *At a Crossroads: "Personhood" and Digital Identity in the Information Society* (Paris, 2007) 10.

13.8 In *Privacy: Concepts and Issues*, we outlined some of the key technological developments that potentially impact on privacy, including:[1059]

- developments relating to computers and digital data, such as advances in computer technology and data collection and analysis;
- developments relating to the internet, such as the collection of personal information online, the availability of personal information and images online and targeted advertising;
- surveillance and location technologies such as visual surveillance and radio frequency identification; and
- technologies of the body, such as biometric and genetic technologies and brain scanning.

We also noted that privacy-enhancing technologies have a role in ensuring that developing technologies offer privacy safeguards.[1060]

FUNCTIONS OF THE PRIVACY COMMISSIONER

13.9 Certain functions of the Privacy Commissioner specifically relate to technological developments. These empower him or her to:[1061]

- inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or *any technical development*, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby;[1062] and
- undertake research into, and to monitor developments in, *data processing and computer technology* to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring.[1063]

13.10 Other generic functions of the Privacy Commissioner are also relevant, such as undertaking educational programmes;[1064] making public statements in relation to any matter affecting the privacy of the individual;[1065] consulting and co-operating with other bodies;[1066] recommending to the Prime Minister legislative or other action;[1067] and recommending to the Prime Minister the acceptance of any international instrument relating to privacy.[1068]

1059 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) chapter 6.

1060 New Zealand Law Commission *Privacy: Concepts and Issues*, (NZLC SP19, Wellington, 2008) paras 6.103–6.120.

1061 The functions of the Privacy Commissioner are also discussed in chapter 6.

1062 Privacy Act 1993, s 13(1)(m).

1063 Privacy Act 1993, s 13(1)(n).

1064 Privacy Act 1993, s 13(1)(g).

1065 Privacy Act 1993, s 13(1)(h).

1066 Privacy Act 1993, s 13(1)(j).

1067 Privacy Act 1993, s 13(1)(p).

1068 Privacy Act 1993, s 13(1)(q).

13.11 The development of new technologies is identified by the Privacy Commissioner to be an important driver for the office's activities: "Monitoring and advising upon technology developments will remain a major priority, given the strong and widespread impact on individual privacy through these changes." [1069]

13.12 Through various forums and networks, the Office of the Privacy Commissioner (OPC) monitors new technologies and reviews their impacts on the protection of personal information.[1070] The Privacy Commissioner also participates in international privacy fora such as the International Working Group on Data Protection and Telecommunications (also known as "the Berlin Group") and the OECD Working Party on Information Security and Privacy (WPISP).

13.13 The Privacy Commissioner's website devotes a section to "You, your privacy and technology", with tips for online privacy, such as privacy pointers for subscribing to online services, shopping online and online banking.[1071] There are also links provided on topics such as government use of biometric technologies; "smart" transport payment systems; social networking online; public attitudes to CCTV camera surveillance; and sensors in everyday life.

13.14 One of the Privacy Commissioner's operating intentions is to assist with achieving improved privacy standards and practice in government and business. A long term impact sought by the OPC is the harnessing of the benefits of technology by New Zealand businesses while better understanding privacy risks and solutions.[1072] Key activities planned include:[1073]

- monitoring and advising on the privacy impacts of proposed legislation, policy and technology initiatives;
- continuing to contribute to and help guide e-government initiatives; and
- publishing additional resources, particularly web-based publications and case notes, including those focusing on technology, privacy and business needs.

13.15 Recent work by the OPC on privacy issues associated with technological developments includes the release of guidance on the use of CCTV cameras,[1074] and a guidance note on the use of portable storage devices in business and government.[1075] The Privacy Commissioner has also produced information about layered privacy notices (including privacy notices for websites)[1076] and a *Privacy Impact Assessment Handbook* (with comments and suggestions particularly suited to projects with a technological component).[1077]

1069 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 9.

1070 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 17. The Privacy Commissioner intends to hold four Technology and Policy Forums in the next operating period.

1071 Office of the Privacy Commissioner www.privacy.org.nz/you-your-privacy-and-technology (accessed 11 December 2009).

1072 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 12.

1073 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 13.

1074 Office of the Privacy Commissioner *Privacy and CCTV: a Guide to the Privacy Act for Businesses, Agencies and Organisations* (Wellington, 2009).

1075 Office of the Privacy Commissioner *Guidance Note on the use of Portable Storage Devices* (Wellington, 2009).

1076 Office of the Privacy Commissioner *Questions and Answers about Layered Privacy Notices* www.privacy.org.nz (accessed 15 January 2010).

1077 Office of the Privacy Commissioner *Privacy Impact Assessment Handbook* (Wellington, 2007).

13.16 The Privacy Act 1988 (Cth) provides for the establishment of a Privacy Advisory Committee, convened by the Australian Privacy Commissioner and made up of government and industry representatives. One member is to have extensive experience in "electronic data processing", which the Australian Law Reform Commission (ALRC) has recommended be changed to experience in "information and communication technologies."[1078] The ALRC has also recommended that the Australian Privacy Commissioner have an express legislative power to establish expert panels as a tool to deal with difficult and emerging areas of privacy regulation, including new and developing technologies.[1079]

13.17 The ALRC has also recommended that the Australian Privacy Commissioner should develop and publish guidance in relation to technologies that impact on privacy,[1080] such guidance to address certain matters including:

- developing technologies such as radio frequency identification (RFID) or data-collecting software such as "cookies";
- when the use of a certain technology to collect personal information is not done by "fair means" and is done in an "unreasonably intrusive way";
- when the use of a certain technology will require agencies and organisations to notify individuals at or before the time of collection of personal information; and
- when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometric systems).

Q155 Do you have any comments on the role and functions of the Privacy Commissioner in relation to technological developments? Should the Privacy Commissioner's functions in relation to technology be revised and should any new functions be added?

Q156 Should the Privacy Act provide for a Privacy Advisory Panel, or empower the Privacy Commissioner to set up expert panels on particular issues, as the Australian Privacy Act does?

1078 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 46.72–46.100, recommendation 46-4(c).

1079 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 46.101–46.108, recommendation 46-5.

1080 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 10-3. See also the recommendations of the Australian Law Reform Commission in relation to biometrics and Privacy Impact Assessments, outlined below.

THE IMPACT OF TECHNOLOGY ON THE PRIVACY ACT FRAMEWORK

13.18 New technological developments create pressure points on the existing Privacy Act framework in a number of key ways. Greater uptake of technological applications has reduced de facto privacy protections such as information being widely dispersed and difficult to access, and limitations on physical storage.[1081] Rapid technological change places increased pressures on personal information handling practices and quickly outstrips conventional information handling techniques.[1082]

13.19 Key privacy principle concepts such as notice and consent may not always be effective in the online environment. Notice in the form of privacy policies is not always user-friendly or sufficiently transparent, and can be easy for users to ignore. Consumers do not always know what they are consenting to, especially regarding secondary uses of their data, and who their data will be shared with.[1083]

13.20 Technology can facilitate vast collections and disclosures of personal information that may affect a large number of people, even though the effects on individuals may be small. Online data collection and use can affect an individual's ability to control his or her personal information without necessarily resulting in demonstrable "harm". While there may sometimes be little measurable harm caused in individual terms, the impact in terms of the societal value of privacy and public confidence may be significant. The Privacy Act's complaints process can only be used if there has been "harm" to the individual concerned;[1084] however, some of the Privacy Commissioner's other functions extend to addressing systemic issues.

Cross-border issues

13.21 Technological changes and the internet pose new challenges for the regulation of agencies that collect, hold or use the personal information of New Zealanders but do not have any physical presence in New Zealand. While "New Zealanders want their personal information protected wherever it travels",[1085] it may be difficult to enforce the New Zealand privacy principles against offshore entities. Issues associated with trans-border data flows are discussed in chapter 14.

Technological neutrality

13.22 The privacy principles are technologically neutral in that they apply to "information", regardless of the form in which it is held.[1086] Thus the legislation is capable of applying to new technologies that enable the collection, use and disclosure of personal information. The Privacy Commissioner has suggested

1081 Senator John Faulkner "Privacy – where do you draw the line?" (Speech to Australian Public Service Commission, Canberra, 8 May 2009).

1082 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 9.

1083 Wendy Davis "Web Privacy Practices Fall Short" (4 June 2009) *Online Media Daily* www.mediapost.com (accessed 26 June 2009).

1084 Privacy Act 1993, s 66. In chapter 8 we propose that the harm threshold for complaints should be removed.

1085 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 14.

1086 Gehan Gunasekara "'MySpace' or Public Space: the Relevance of Data Protection Laws to Online Social Networking" (2008) 23 NZULR 191, 198.

that the rate of technological change favours retaining technologically neutral principles, to reduce the need for constant updating of legislation in the face of new developments.[1087]

13.23 Nevertheless, the adequacy of existing data protection safeguards as applied to the emerging information society is being questioned.[1088] It has been suggested that privacy rights in the online environment are diluted, inadequately protected and difficult to enforce.[1089] The privacy principles are based on OECD guidelines developed in the 1970s. At that time, when the internet was in a state of relative infancy, the key privacy concerns related to issues associated with databases.[1090] The rapid rate of technological change since then raises the question of whether the concept of technological neutrality, as embedded in the privacy principles, remains effective, or whether it has been somewhat eclipsed, given the variety of ways in which information about individuals and their activities can now be collected, aggregated, stored, used and re-used.

13.24 The ALRC has concluded that it would be undesirable to recommend significant changes to the Australian Privacy Act's privacy principles to accommodate technologies which are yet to be invented or deployed, and that, where possible, provisions of the Privacy Act should be technology neutral.[1091] However, the ALRC did not foreclose the possibility of technology-specific regulation in certain circumstances, such as through codes of practice.[1092]

The global context

13.25 Because of the cross-border nature of the internet and the information handling practices that it gives rise to, we do not see that it is practical to try to formulate significant reforms to New Zealand's Privacy Act framework in isolation from international responses and regulatory practices. New Zealand is a relatively small participant in the international marketplace and its influence on global practices is limited. It would make little sense for New Zealand to strike out and establish a particular approach to technology-related privacy issues that is out of step or incompatible with the approaches of more influential jurisdictions, or approaches endorsed by regional or co-operative blocs such as the EU, APEC and the OECD.[1093] While it remains important for New Zealand to maintain a robust privacy framework to regulate domestic privacy issues related to technological developments, reform also needs to be mindful of the international context.[1094]

1087 *Necessary and Desirable* 17.

1088 OECD Directorate for Science, Technology and Industry *At a Crossroads: "Personhood" and Digital Identity in the Information Society* (Paris, 2007) 6.

1089 Office of the Privacy Commissioner (Cth) *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (Sydney, 2005) para 8.2, citing submission of Electronic Frontiers Australia.

1090 *Necessary and Desirable* 15–16.

1091 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 10.9.

1092 See for example the Biometrics Institute Privacy Code approved by the Australian Privacy Commissioner.

1093 See *Necessary and Desirable* 17. See discussion of the approaches of the EU, APEC and the OECD in chapter 14.

1094 See chapter 14.

13.26 New Zealand policy can be informed by international efforts to address technology-related privacy issues. International organisations and privacy regulators devote significant effort and resources to debating and proposing reforms. New Zealand citizens also benefit indirectly from the actions of overseas privacy regulators. Where challenges to practices result in improved privacy standards, this may benefit the global community, not just users in the privacy regulator's home jurisdiction.[1095]

Q157 Is the basic framework of the Privacy Act adequate to deal with technological change? Should the privacy principles remain technologically neutral?

THE INTERNET AND THE PARTICIPATORY WEB 2.0

13.27 In this section we outline issues arising through the use of search engines, websites and social networking sites such as Facebook, MySpace, and Bebo. The internet and the possibilities it has brought with it pose challenges for the privacy of individuals. The World Wide Web is constantly adapting and its limits continue to expand. Websites are now more accessible and allow for an increasingly inter-active experience. New Web 2.0 sites give users greater control over the content of pages, allowing them to upload their own information, add to pre-existing information, and interact with the information of others. These sites include blogs, social networking sites and other sites such as Flickr and YouTube that allow users to upload their photos and videos for others to access.

13.28 In *Privacy: Concepts and Issues*, we observed that New Zealanders are enthusiastic users of the internet.[1096] The authors of *The Internet in New Zealand* found that 78 per cent of New Zealanders use the internet.[1097] The same study showed that New Zealanders spend a large number of hours on the internet for personal, non-work-related purposes.[1098] Other research has shown that our common internet activities include general Web surfing or browsing, internet banking, searching for information on goods and services, and listening to music.[1099]

1095 For example, see the Canadian Privacy Commissioner's investigation into Facebook, discussed below.

1096 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008), para 6.22.

1097 A Bell and others *The Internet in New Zealand 2007: Final Report* (Institute of Culture, Discourse and Communication, AUT University, Auckland, 2008) 3. Of the 22 per cent that are not users, six per cent are ex-users, and only sixteen per cent have never used the internet.

1098 A Bell and others *The Internet in New Zealand 2007: Final Report* (Institute of Culture, Discourse and Communication, AUT University, Auckland, 2008) 3.

1099 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.

13.29 OPC's website offers internet users guidance about their personal privacy and the internet with information about how personal information is collected by websites and search engines, and what users can do to prevent or mitigate any privacy harms that may arise through the use of the internet.[1100] The website notes that the Privacy Act does not generally apply to non-New Zealand agencies. This highlights the Privacy Commissioner's limited jurisdiction to act in relation to data handling practices that occur outside New Zealand.

13.30 Personal information handling in an online environment can give rise to various Privacy Act issues including:

- whether online information is "personal information" for the purposes of the Privacy Act;[1101]
- whether the information is "publicly available information" within the exception to the collection, use and disclosure principles;
- whether privacy policies are adequate so that acceptance can be considered to constitute consent to data handling practices for purposes of the privacy principles;[1102]
- whether the access and correction principles apply or whether the data collection is outside the scope of the Privacy Act; and
- whether the Privacy Act complaints process is available or whether any interference with privacy occurred outside New Zealand and is therefore outside the scope of the Privacy Commissioner's authority to act.[1103]

13.31 One issue fundamental to the interface between users and the online environment is identity management. The Information and Privacy Commissioner of Ontario has issued a report on this topic, suggesting that debate is needed about the development of mechanisms to assure the security and privacy of identity information:[1104]

> Almost all online activities, such as sending emails, filing tax declarations, managing bank accounts, buying goods, playing games, connecting to a company intranet, and meeting people in a virtual world, require identity information to be given from one party to another. Today, most users have to establish their identity each time they use a new application, usually by filling out an online form and providing sensitive personal information (e.g. name, address, credit card number, phone number etc.).
>
> A typical Internet user in Canada has provided some type of personal information to dozens of different websites. If you count cookies and IP addresses as personal information, then Internet users have left behind personally identifiable information everywhere they've been. They have left "digital bread crumbs" throughout cyberspace – and they have little idea how that data might be used or how well it is protected.

1100 See Office of the Privacy Commissioner "You, Your Privacy and Technology" www.privacy.org.nz/you-your-privacy-and-technology (accessed 11 December 2009).

1101 This may be problematic where individual pieces of information can be brought together from various internet sources which in aggregated form may comprise of personal information.

1102 See Alan Toy "Consent to Online Privacy Policies" (2009) 15 NZBLQ 235.

1103 See chapter 14 on cross border issues.

1104 Ann Cavoukian, Information and Privacy Commissioner of Ontario *Privacy in the Clouds, A White Paper on Privacy and Digital Identity: Implications for the Internet* (Toronto, 2008) 9.

The report suggests that what is needed is flexible and user-centric identity management, so that through informed consent, individuals have better control over their personal information that is used for identity authentication purposes, as well as reducing the risk of identity fraud and the potential for online surveillance and profiling.

Search engines and websites

13.32 As we outlined in *Privacy: Concepts and Issues*, there is an abundance of information that can be collected about individuals from their online activities such as using search engines and visiting websites.[1105] Data is provided by internet users both consciously (for example, registering on websites) and unconsciously (for example, search terms and click stream data). The incentive to collect online data derives from its usefulness both for website design, customisation and maintenance, and for the purpose of online targeted advertising.[1106] In the public sector, internet data is collated for understanding and optimising web usage.[1107]

13.33 Through technical means such as the use of cookies,[1108] search engines collect the terms typed into a search engine by an individual user, the IP address of the user's computer, "click stream data", and a unique identifier for the user's web browser.[1109] Search engines can also collect the personal information of users required to sign in to be able to use particular services, such as email.[1110]

13.34 Click stream data is collected by search engines in the form of search histories, as well as by web site operators and third party advertisers and trackers through the placement of tracking cookies on the user's machine and the use of web bugs,[1111] a process which is largely invisible to users. In the private sector, collected data may then be shared with affiliate entities, or sold and purchased between site operators to enhance profiles.[1112]

13.35 Search engines also enable users to pull together information about an individual from all over the internet, creating a full and sensitive picture of that individual. In this regard it has been noted that: "The personal information a user posts online, combined with data outlining the user's actions and interactions with

1105 New Zealand Law Commission *Privacy: Concepts and Issues*, (NZLC SP19, Wellington, 2008) paras 6.24–6.30.

1106 Targeted advertising is discussed in more detail in chapter 15.

1107 Center for Democracy & Technology and Electronic Frontier Foundation *Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites* (Washington, DC, 2009) 1.

1108 "Cookies" are small pieces of code that some web sites place in the computer hard drive of users who visit the website. Cookies collect header information about the visitor and may include click stream data and may also record any information that a user is requested to supply to a website: New Zealand Law Commission *Electronic Commerce Part Three – Remaining Issues* (NZLC R68, Wellington, 2000) 25.

1109 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.26.

1110 Two common examples include Google and Yahoo which offer both email and search services.

1111 For discussion of web bugs see UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 8. The study concluded that web bugs are ubiquitous on the web.

1112 For example, Google has five web trackers: Analytics, DoubleClick, AdSense, FriendConnect, and Widgets.

other people, can create a rich profile of that person's interests and activities."[1113] The ability to access so much information about people may increase their chances of becoming victims of identity theft or fraud.[1114]

Privacy issues

13.36 The internet has undoubtedly brought huge benefits to business, government and the individual citizen. But it also poses numerous privacy challenges for individuals. Search engines and websites collect and monitor the personal information of users, often when the user is unaware that this is occurring. This information can be retained indefinitely, with limited or no benefit for the user. Although much of it is anonymised, information may be tracked back to an individual user through his or her IP address.[1115] Consent to collect personal information is not always sought in a transparent way.

13.37 One view is that the online collection of personal data is simply the corollary of the collection of offline data: "At least when I am online I assume that I am being tracked, and frankly, I don't care."[1116] But when asked about online privacy, most people say they want more information about how they are being tracked and more control over how their personal information is used.[1117] In a 2008 survey commissioned by the OPC, 82 per cent of respondents were concerned (including 62 per cent very concerned) about the "security of personal information on the internet" and two-thirds said they were uncomfortable about internet search engines and social networking sites tracking internet use and emails in order to deliver targeted advertising.[1118] According to one study:[1119]

> There is overwhelming evidence from various surveys to show that users are concerned about the collection of data by websites. These surveys also show that users desire control of who can collect or see data about them and for what purposes. However, despite these concerns and desires, the studies also show that users are often ignorant of how data collection works, whether it is within the scope of the law and how to stop it.

13.38 Some of the information that is collected by search engines and websites is capable of being used to identify an individual person. IP addresses are the primary means by which information submitted to web sites and search engines

1113 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 4.

1114 Identity theft is discussed in chapter 17.

1115 For discussion of the limits of anonymisation to protect informational privacy, see Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (University of Colorado Law Legal Studies Research Paper No 09–12, 2009).

1116 George Simpson "I'm Being Followed and I Don't Care" (25 June 2009) *Online Media Daily* www.mediapost.com (accessed 26 June 2009). See also Wendy Davis "How Much Targeting is Too Much?" (24 June 2009) *Online Media Daily* www.mediapost.com (accessed 26 June 2009).

1117 Miguel Helft "Google is Top Tracker of Surfers in Study" (2 June 2009) http://bits.blogs.nytimes.com (accessed 24 February 2010).

1118 Office of the Privacy Commissioner *Individual Privacy and Personal Information Survey 2008* www.privacy.org.nz (accessed 13 January 2010).

1119 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 17.

becomes personally identifiable.[1120] This information can also be tracked back to individual users or computers through analysing the search terms individuals enter into computers (including "vanity" searches which involve individuals using search engines to seek out information about themselves held on the internet), and through the use of cookies. Some cookies are beneficial to users; for example, they may configure a news page in a manner that a user has requested during a previous visit. But they also carry privacy concerns for individuals. Users are rarely aware that cookies are being placed on their hard drives by any particular website, limiting the ability to give informed consent to the collection practices of a particular site.

13.39 Of primary concern is the lack of transparency around the collection, retention and use of the personal information. Most users are unaware that search engines and websites are collecting their personal information and the purposes this information is being collected for. Users are therefore unable to give informed consent to the collection, retention, and use of their personal information.

13.40 Also of concern is the reduced ability individuals have to control the use of their personal information once it is available on the internet. Indeed, it was observed at a conference of data protection and privacy professionals that:[1121]

> As with all information uploaded onto the internet the risks for an individual's privacy are increased as the ability to control one's information diminishes the longer something exists in an open and readily accessible format. For this reason the dissemination of information on the internet differs from dissemination to a group of friends in the real world. The "community" that exists on the internet includes millions of subscribers and an individual has little control over who can gain access to their personal information.

13.41 The ability for search engines to log information about users such as the search terms they use, their click stream data, or their locations through their IP addresses, has led to a rise in "behavioural marketing".[1122] Individual pieces of information a person enters into a search engine over time, when aggregated and monitored, can build up a substantial record of personal information about an individual, including political affiliations, sexual preferences, and religious beliefs. Marketers make use of these characteristics to shape marketing practices and advertisements in a manner that will maximise their chances of profiting from consumers. Of concern is the opaque nature of practices used in behavioural marketing that result in "consumers remaining largely unaware of the monitoring of their online behaviour, the security of this information and the extent to which this information is kept confidential."[1123]

1120 Electronic Privacy Information Center "Search Engine Privacy" www.epic.org/privacy/search_engine (accessed 10 December 2009). There are a range of views as to whether IP addresses are personal information within the scope of the Privacy Act. This issue is discussed in chapter 3.

1121 Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 30 October 2008).

1122 Behavioural marketing is discussed in chapter 15.

1123 Electronic Privacy Information Center "Search Engine Privacy" www.epic.org/privacy/search_engine (accessed 10 December 2009).

13.42 Researchers at the University of California at Berkeley have published a study regarding the data handling practices of popular websites and the concerns of internet users with a view to identifying the gap between users' expectations and practice, a gap they found to be a wide one.[1124] Based on previous studies and surveys that had been conducted the researchers observed that:[1125]

- users are concerned about websites collecting information about them and using it for behavioural advertising;
- users desire control over the collection and use of information about them; and
- users lack knowledge and understanding about data collection practices and policies.

To alleviate these concerns and to give individuals more control over their personal information the researchers made the following recommendations:[1126]

- users should be entitled to see all data collected about them and who their data has been shared with;
- users should be given clear and proper notice as to who their data will be shared with and data should only be shared with prior permission;
- third party tracking should be made more transparent and browser developers should provide a function that alerts users to the presence of third party trackers;
- the Federal Trade Commission[1127] should become more aggressive in protecting privacy on the internet;
- privacy policies should be readable for average users; and
- enhancement (buying information about users from outside sources) should be subject to user opt-in.

13.43 The Article 29 Data Protection Working Party[1128] has also reported on data protection issues related to search engines. The group found that the collection and storage of search histories of individuals in a directly or indirectly identifiable form invokes the protection individuals are afforded under Article 8 of the European Charter of Human Rights to respect for private and family life.[1129] Accordingly the EU Data Protection Directive applies to the processing of personal data by search engines (including IP addresses).[1130] Essentially, the recommendations support general calls for greater transparency of information collection practices and the need for pre-informed consent to the collection of personal information. The recommendations include:

- that personal data should be retained no longer than necessary, and should only be kept in any case if there is a reason to do so;

1124 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009).

1125 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 5.

1126 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 5.

1127 The US government regulator responsible for enforcing consumer privacy issues.

1128 The Working Party is an independent European advisory body on data protection and privacy.

1129 Article 29 Data Protection Working Party *Opinion on data protection issues related to search engines* (4 April 2008) 00737/EN WP148, 7.

1130 Article 29 Data Protection Working Party *Opinion on data protection issues related to search engines* (4 April 2008) 00737/EN WP148, 8.

- that users should be informed when they are visiting websites that use cookies,[1131] and that cookies should only be used in any case for a reasonable period of time (rather than permanently or for unnecessarily long periods);
- that websites should provide sufficient information to users (through transparent privacy policies) to enable them to make informed choices about their internet use; and
- that websites should allow users access to the personal information that the site holds about them, including the ability to delete and correct any erroneous information.

13.44 In the United Kingdom, the Information Commissioner is engaging in consultation on a code of practice to provide comprehensive, accessible guidance on the following broad areas:

- operating a privacy-friendly website;
- rights and protections for individuals;
- privacy choices and default settings; and
- cyberspace and territoriality.

The code is due to be released in May 2010.[1132] The Information Commissioner has also released a code of practice about privacy notices, with examples of good and bad privacy notices.[1133]

13.45 The New Zealand Privacy Commissioner has also produced information about privacy notices.[1134] The New Zealand Computer Society Code of Practice encourages information technology professionals to consider privacy issues such as privacy notices when creating websites.[1135]

13.46 Some search engines and websites have started to respond to concerns of privacy advocates and created tools aimed at allowing individuals to gain greater control over their personal information. One such service, known as Google Dashboard,[1136] allows users who hold Google accounts to view a summary of any information the site holds about them and enables them to delete it if they choose to do so.[1137] It is said that the site provides an answer to the question "what does Google know about me?"[1138] Google claims that Dashboard gives users more transparency and control over their use of Google products, including Google search.[1139] Tools such as this go some way towards ensuring that individuals

1131 An amendment to the EU privacy directive requires user consent to the use of cookies: "EU Adopts Law Requiring User Consent for Cookies" (10 November 2009) www.clickz.com (accessed 10 December 2009); "Browser Settings Satisfy New EU Cookie Law, says IAB" (8 December 2009) www.clickz.com (accessed 10 December 2009).

1132 Information Commissioner's Office (UK) "Our Current Consultations" www.ico.gov.uk (accessed 27 November 2009).

1133 Information Commissioner's Office (UK) *Privacy Notices Code of Practice* (2009).

1134 Office of the Privacy Commissioner *Questions and Answers about Layered Privacy Notices* www.privacy.org.nz (accessed 15 January 2010).

1135 New Zealand Computer Society *Information Technology Code of Practice* (2009).

1136 Google Dashboard www.google.com/dashboard (accessed 18 January 2010).

1137 The site also allows users to review and regulate information about a user created through the use of other Google products. These include Gmail, YouTube, and Google docs.

1138 http://googlesystem.blogspot.com/2009/11/google-dashboard.html (accessed 10 December 2009).

1139 http://googleblog.blogspot.com/2009/11/transparency-choice-and-control-now.html (accessed 10 December 2009).

maintain control and awareness of how their search history is tracked and recorded. Critics of Dashboard consider that although this is a step in the right direction, it should give users total ability to be anonymous from the company and advertisers in areas such as search data and online behaviour.[1140]

The public sector

13.47 In the US, the Center for Democracy & Technology and the Electronic Frontier Foundation have issued "open recommendations" for government agencies to balance the key role that the internet has to play in citizen engagement and the privacy of citizens who engage through the site.[1141] The paper recommends that agencies should only be allowed to use "Web measurement" (the analysis of internet data in the aggregate to understand and optimise web usage) if certain conditions are observed:

- Web measurement data should only be used for that purpose;
- agencies should avoid outsourcing data collection to commercial partners;
- disclosure about the use of Web measurement tools should be made in privacy policies;
- the collection of data for cross-session measurement (requiring persistent user identifiers such as persistent cookies that last across sessions) should be subject to user choice;
- individual-level data collected for measurement purposes should be retained for no more than 90 days, while elements of individual-level data that are not relevant to measurement analysis and reporting should be deleted as soon as possible after collection;
- privacy compliance procedures should be independently verified; and
- persistent tracking technologies (such as cookies) should be subject to further conditions, including a compelling need to gather the data, and appropriate privacy safeguards.

13.48 No legal controls restricting the use of cookies on government websites exist in New Zealand. At a minimum, the New Zealand Government Web Standards 2.0 require that users of government websites be informed if a site is using cookies and the implications of their use.[1142] The standards also provide that the privacy statement (which a site is required to have) should clearly state the agency's policy regarding the collection and use of statistical information including the use of users' IP addresses.[1143] Similarly, the use of cookies and tracking of click stream data is not prohibited in Australia at the federal level. The Australian Privacy Commissioner's website states that if federal government websites do use cookies and track click stream data, users are to be fully informed of this and the possible implications.[1144]

1140 See, for example, comments in Doug Gross "Google Releases Dashboard Privacy Tool" (6 November 2009) http://edition.cnn.com (accessed 24 February 2010).

1141 Center for Democracy & Technology and Electronic Frontier Foundation *Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites* (Washington, DC, 2009).

1142 New Zealand Government *Web Standards 2.0* (Wellington, 2009).

1143 New Zealand Government *Web Standards 2.0* (Wellington, 2009).

1144 Office of the Privacy Commissioner (Cth) *Guidelines for Federal and ACT Government Websites* (Sydney, 2003).

Social networking

13.49 In *Privacy: Concepts and Issues*, we discussed the prevalence of social networking, particularly among young people.[1145] Social networking sites such as MySpace, Bebo, and Facebook can be described as "websites that let people socialise online; send messages to one another; share interests and information; chat; meet people; and post information, photos and videos about themselves for others to look at."[1146] Social networking has been described as "the global consumer phenomenon of 2008",[1147] with social networking and blogging sites now the fourth most popular activity on the internet.

13.50 Social networking sites allow individuals to create a personal account that is accessible by user name and password. Accounts can usually be created after providing a name and email address but in some cases more information, including gender and date of birth details, may also be required. All other information is uploaded voluntarily by the individual user, including information such as telephone numbers and physical and email addresses. In doing so a user creates an online identity for himself or herself and gains the ability to communicate with other individuals who have similarly created their own identities on the network. Once an account is created the information is accessible to other users of the social networking site and, if users do not take the necessary steps to restrict access to their information, can be accessible to anyone using the internet. Some sites offer security settings which allow users to restrict access to others; however this is rarely the default position.

13.51 Social networking sites contribute to the vast wealth of personal information about individuals that is amassing on the internet.[1148] A 2007 study found that of the 78 per cent of New Zealanders who use the internet, 28 percent are actively engaged in social networking every week.[1149] According to another study conducted in 2008, 57.5 per cent of internet users worldwide use social networking sites.[1150]

13.52 Social networking sites are generally free to users,[1151] and gain much of their revenue through advertising, which appears as part of an account page accessed by the individual user. As well as providing advertisers with a marketing

1145 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 5.33–5.48.

1146 Office of the Privacy Commissioner (Cth) "What Are Social Networking Sites?" www.privacy.gov.au/faq/individuals/sn-q1 (accessed 10 December 2009).

1147 Nielsen *Global Faces and Networked Places: a Nielsen Report on Social Networking's New Global Footprint* (2009) 1.

1148 For example, Facebook reports that it has more than 300 million active users worldwide, that more than 2 billion photos, and 14 million videos are uploaded onto the site each month and that more than 2 billion pieces of content (such as weblinks, news stories, blog posts, notes and photos) are shared with other users each week: "Statistics" www.facebook.com/press/info.php?statistics (accessed 10 December 2009).

1149 A Bell and others *The Internet in New Zealand 2007: Final Report* (Institute of Culture, Discourse and Communication, AUT University, Auckland, 2008) i.

1150 Study by Universal McCann Agency, 2008, cited in Trans Atlantic Consumer Dialogue "Resolution on Social Networking" (INFOSOC 39-09, London, 2009).

1151 However users of social networks may in fact "pay" through secondary uses of their personal profile data by the service providers, for example for targeted marketing: International Working Group on Data Protection in Telecommunications *Report and Guidance on Privacy in Social Network Services – Rome Memorandum* (43rd Meeting, Rome, 3–4 March 2008) 2.

platform, some sites repackage and sell the information of users to third parties for marketing and business purposes. Many sites sell this information in an anonymised or aggregated form that strips the information of individually identifiable factors.

Privacy issues

13.53 While social networking sites provide individual users with a new means of communication and opportunities to interact with others at the touch of a button, these sites carry risks for the privacy of individuals, both users and non-users, whose information is uploaded or used without consent. Social networking sites give rise to general internet-related privacy issues (discussed above) as well as additional privacy issues including:

- the fair use of personal information by social networking sites, other individuals and third party application developers;
- the potential for profiling individuals by piecing together pieces of information available on the internet;
- the sensitive nature of information uploaded by individual users with inadequate privacy settings;
- lack of knowledge amongst users about what is, and what is not, restricted from access by other users and third parties, and whether privacy policies are sufficiently transparent;
- the lack of privacy-friendly and security-enhancing default settings; and
- the particular privacy implications for certain groups such as children.

Privacy settings

13.54 Privacy settings available differ from site to site. Certain social networking sites allow individuals to choose whether or not personal information is shared with others. Some sites offer a granulated security regime whereby individuals can choose whether particular information is available to different grades or groups of people. Users may choose to allow their "friends" group access to their personal photographs, but not allow access to anyone in their "family" group. Privacy groups have voiced concern that privacy-friendly settings are often not the default settings on social networking sites.[1152] This means that an individual must actively set their security settings in a privacy-friendly manner. Some sites, such as Facebook, have taken measures to reduce the privacy risks for individual users who access their sites.[1153]

1152 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 7.

1153 Facebook, for example, has stated that "Facebook's privacy settings have played a central part in giving users control over who has access to their personal information by allowing them to choose the friends they accept and networks they join… In addition … users are given extensive and precise controls that allow them to choose who sees what among their networks and friends, as well as tools that give them the choice to make a limited set of information available to search engines and other outside entities." Office of the Privacy Commissioner of Canada *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc* (PIPEDA Case Summary #2009-008, Ottawa, 2009) para 66.

Information sharing

13.55 The underlying premise of social networking sites is the sharing of information with others. When information is uploaded onto the internet, without control, this can be viewed, downloaded, manipulated and collected by people worldwide. Unauthorised release of this information can be harmful to the individual concerned.[1154] Employers, for example, have been known to access social networking pages before hiring prospective staff, and decline certain applicants on the basis of what they find. A Canadian woman is reported to have lost her long term sickness benefit due to her insurance company discovering photographs on Facebook that suggested she did not have the injury she claimed to have.[1155] Social networking sites are now also being monitored by debt collection agencies to search for individuals who have disappeared leaving large debts.[1156]

13.56 As we noted in *Privacy: Concepts and Issues*, the privacy principles do not apply to the use and disclosure of personal information that is contained in or sourced from "a publicly available publication",[1157] 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." Whether information posted on a social networking site amounts to a publication that is generally available to members of the public may depend on the privacy settings involved.

13.57 As well as divulging one's own personal information on social networking sites, the personal information of other people is increasingly being uploaded and being made available without consent, for example, by uploading photographs or written postings that disclose information about other people.[1158] An individual affected by someone else's disclosure, if it is particularly serious, may be able to bring a civil claim for a breach of privacy against the individual who uploaded the personal information.[1159]

13.58 There is also the possibility that an affected individual could make a complaint to the Privacy Commissioner. However, as we noted in *Privacy: Concepts and Issues*,[1160] section 56 of the Privacy Act provides that the privacy principles 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." The primary users of social networking sites are generally individuals who do so to share information with acquaintances,

1154 In *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.35–6.40 we noted the particular issues that arise with images on the internet. See also David V Richards "Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by § 230 of the Communications Decency Act" (2007) 85 Tex L Rev 1321.

1155 "Depressed woman loses benefits over Facebook photos" (21 November 2009) *CBC News* www.cbc.ca (accessed 10 December 2009).

1156 John Silvester "Policing in the internet age" (16 November 2009) www.stuff.co.nz (accessed 10 December 2009).

1157 New Zealand Law Commission *Privacy: Concepts and Issues*, (NZLC SP19, Wellington, 2008) para 6.43.

1158 See New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.33.

1159 For discussion of the tort of disclosure of private facts, see New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2009).

1160 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.43.

friends and family, although there are sites used for professional networking. Section 56 may therefore limit the extent to which the privacy principles apply in this context.[1161]

Third party access

13.59 As well as providing a basis for sending messages and uploading photographs, some social networking sites provide third party applications for users. Third party applications are tools accessible through the social networking platform for the enjoyment and benefit of users. These include games and quizzes, match-making tools, horoscopes, birthday calendars, count-down timers, and virtual pets. In the case of Facebook, the website states that it has more than one million developers and entrepreneurs from more than 180 countries who develop applications for the site and that more than 350,000 applications currently exist on the site.[1162] One concern is the ability of developers of third party applications to access without notice the personal information of those who use the applications.

13.60 There is also concern regarding third party use of personal information generally, whether information is obtained through third party applications, with the authorisation of non-transparent privacy policies, through malicious acts to gain access to supposedly secure information, or through unauthorised use more generally, such as unauthorised use of information posted by a user's friends. Personal data published on social networking sites can be used by third parties or other users to create profiles for a wide variety of purposes, including commercial purposes, and major risks include identity theft,[1163] financial loss, loss of business or employment opportunities and physical harm.[1164]

Research and policy responses

13.61 In response to privacy concerns relating to social networking, several bodies have conducted studies and issued recommendations for social networking sites about how they can protect the privacy interests of users and comply with privacy laws in various countries.

13.62 A resolution on privacy protection in social network services was passed at the 2008 Conference of Data Protection and Privacy Commissioners, which contained a number of recommendations for providers and users of social networking services.[1165] The Conference considered that "providers of social network services have a special responsibility to consider and act in the interests of the individuals using social networks."[1166] To meet the requirements of data protection laws, it resolved that that social network services should:

1161 See discussion of section 56 in chapter 5.

1162 Facebook "Statistics" www.facebook.com/press/infor.php?/statistics (accessed 10 December 2009).

1163 Identity theft is discussed in chapter 17.

1164 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163.

1165 Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 30 October 2008).

1166 Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 30 October 2008) 3.

- respect the privacy standards of the countries where they operate their services;
- provide information to users about the use of their information by the social network, privacy and security risks, as well as guidance on how users should handle their own information and the information of other people on the social networking site;
- improve user control over profile data and secondary use of profile and traffic data (including by third party developers);
- offer privacy-friendly default settings;
- offer pseudonymous profiles as an option;
- prevent bulk downloading of profile data by third parties; and
- offer non-indexability of profiles by search engines as a default setting.

13.63 The Article 29 Data Protection Working Party has made a series of further recommendations, including that:[1167]

- sites should contain a link to a complaints body responsible for privacy issues in the country concerned; and
- sites should maintain policies to retain data on inactive users for finite periods and agree to delete the data of abandoned accounts.

The Working Party found much social networking will fall within the "household exemption" to the Data Protection Directive;[1168] however, where user activities extend beyond a purely personal or household activity, for example, to advance commercial, charitable or political goals, the exception does not apply, and data protection restrictions will apply to the use of personal information derived from social networking sites. The Working Party suggested that a high number of contacts could be an indication that the exception does not apply.[1169]

13.64 A resolution on social networking was passed by the Trans Atlantic Consumer Dialogue (TACD), a forum of US and EU consumer organisations, resolving that US and EU governments should pass legislation regulating social networks; improve co-operation and enforcement; and raise awareness of privacy risks. The TACD also resolved that social network operators should integrate privacy and security by design; enable consumers to remain "masters of their data"; develop industry and ethical codes; and provide advertisement and tracking-free versions.[1170]

13.65 In 2009 a set of "Safer Social Networking Principles" were signed between the European Commission and a number of social networking sites including Facebook, MySpace, and Bebo. The principles were developed to provide good practice guidelines (such as default privacy settings) to providers of social networking and interactive sites (such as Google) with a particular view to minimising harms to children and young people.

1167 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 12–13.

1168 The New Zealand equivalent is the "domestic affairs" exemption in section 56 of the Privacy Act.

1169 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 6.

1170 Trans Atlantic Consumer Dialogue "Resolution on Social Networking" (INFOSOC 39-09, London, 2009).

13.66 In 2008 the Privacy Commissioner of Canada commenced an investigation into the practices and policies of Facebook in response to a complaint made by the Canadian Internet Policy and Public Interest Clinic.[1171] The issues involved included the site's default privacy settings, collection and use of users' personal information for advertising purposes, disclosure of users' personal information to third party application developers, and collection and use of non-users' personal information

13.67 The Commissioner's Office issued a report including 20 recommendations for changes to Facebook's practices to comply with the privacy laws of Canada. Facebook ultimately agreed to all of the recommendations made and undertook to change its global policies and practices to comply,[1172] including:

- allowing individual users to retain more control over what information they disclose to third party applications;
- making changes to account deactivation and deletion terms and practices;
- making provision for the accounts of deceased users; and
- changes that protect the privacy interests of non-users.

13.68 Facebook has also responded to pressure from users by altering information retention and sharing practices and improving privacy controls. The site now gives members comment and voting rights over how the site is governed.[1173]

CLOUD COMPUTING

13.69 Cloud computing describes the trend towards accessing computing and storage facilities from service providers on the internet, instead of using packaged software, and dedicated hard drives or network servers:[1174]

> Cloud computing represents a new way to deploy computing technology to give users the ability to access, work on, share, and store information using the Internet. The cloud itself is a network of data centers – each composed of many thousands of computers working together – that can perform the functions of software on a personal or business computer by providing users access to powerful applications, platforms, and services delivered over the Internet.

The result of this trend is that "We are using less data and software that sit on our hard-drive and spending more time in our web browsers accessing data and applications that stream through the web."[1175] Data stored in the cloud can include information contained in word processing documents and other business documents, employee records, health information, tax and accounting records, schedules, calendars and contacts.[1176]

1171 Office of the Privacy Commissioner of Canada *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc* (PIPEDA Case Summary #2009-008, Ottawa, 2009).

1172 Office of the Privacy Commissioner of Canada "Facebook agrees to address Privacy Commissioner's concerns" (27 August 2009) News Release.

1173 Nielsen *Global Faces and Networked Places: a Nielsen Report on Social Networking's New Global Footprint* (2009) 9.

1174 Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) ii.

1175 "Microsoft after Bill Gates" (26 June 2008) *The Economist*, quoted in Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) 5.

1176 Shari Claire Lewis "Cloud Computing Brings New Legal Challenges" (8 July 2009) New York Law Journal.

13.70 The advantages of cloud computing include its convenience and versatility, with a shift from using an anchored, traditional personal computer terminal for internet services to using a range of smaller portable computing devices for internet access (such as internet capable cellphones).[1177]

13.71 Cloud computing can involve individuals using cloud services in relation to their personal information, as well as businesses using cloud services for their operations that may include the handling of the personal information of their employees, clients or customers. According to the Electronic Privacy Information Center, as of September 2008, 69 per cent of Americans were using webmail services, storing data online and otherwise using software programmes such as word processing applications whose functionality is located on the web.[1178] Popular cloud services used by individuals include web mail, social networking sites, photo sharing and video viewing sites such as YouTube.[1179]

13.72 Cloud computing is of growing importance to businesses as it offers efficiencies and cost savings from outsourcing IT functions such as computing and data storage through access to the significant capacity of data centres.[1180] Users can access this computing power in a similar way to utilities such as electricity, and pay for the service they use, thereby saving the cost of unused capacity: "A key underlying premise of the economic model driving cloud computing is that sharing resources creates efficiencies."[1181]

13.73 The term "cloud computing" covers a range of different services that are organised in different ways.[1182] The foundation of all Cloud services is Infrastructure as a Service (IaaS):[1183]

> The capability provided to the consumer is to rent processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer

1177 See Jonathan Zittrain "Lost in the Cloud" (20 July 2009) *New York Times* www.nytimes.com (accessed 22 July 2009).

1178 Electronic Information Privacy Center "In re Google and Cloud Computing" http://epic.org/privacy/cloudcomputing/google (accessed 17 June 2009).

1179 Jeffrey F Rayport and Andrew Heyward Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) i.

1180 For example it has been estimated that a proposed move to Google Apps by the Los Angeles City Council would save about US$13 million in software licensing and personnel costs over a 5 year period: Jaikumar Vijayan "Google Defends Google Apps Security" (28 July 2009) *ComputerWorld* www.computerworld.com (accessed 31 July 2009). See also the NZ Post three-year cloud computing contract for Google email and messaging that will save NZ$2 million: Anthony Doesburg "NZ Post Signs Up for Cloud Service" (21 July 2009) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 23 July 2009).

1181 Jim Reavis, Pam Fusco and Josh Zachry "Data Center Operations" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 59.

1182 The US National Institute of Technology and Standards has produced a draft working definition of cloud computing as "a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The five key characteristics are (i) on-demand self-service, (ii) ubiquitous network access (iii) location independent resource pooling (iv) rapid elasticity and (v) measured service: see Katten Muchin Rosenman LLP and UHY Advisors FLVS Inc *Cloud Computing: Practice Safe SaaS: Don't Lose Your Head (or Data) in the Clouds* (2009).

1183 Christofer Hoff "Cloud Architecture" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 17.

does not manage or control the underlying cloud infrastructure but has control over operating systems, deployed applications, and possibly select networking components (e.g. firewalls, load balancers).

This foundation can be built on by other delivery models such as Platform as a Service (PaaS)[1184] and Software as a Service (SaaS).[1185]

13.74 In addition, there are four primary ways in which Cloud services can be deployed and characterised:[1186]

- Private Clouds, which are dedicated to a single organisation, either on their premises or off their premises;
- Public Clouds, which are provided to a single organisation or multiple organisations, generally off premises;
- Managed Clouds where the physical infrastructure is owned by or physically located in an organisation's data centre with aspects of management and security controlled by the service provider; and
- Hybrid Clouds which are a combination of public and private clouds.

13.75 The rapid growth in these services has given rise to some security glitches that have allowed private information to be shared without authority.[1187] Use of these services may involve a privacy trade-off where a service provider offers a free service such as storage, while retaining the right to mine user data for market research or for the purposes of targeted advertising.[1188] In some cases, users have found it difficult to regain or erase their data when they wish to terminate their use of one of these services.

13.76 Because cloud computing can involve the transfer of data and potentially a reduction or loss of control by the organisation which is the ostensible custodian of that information, it gives rise to a range of issues,[1189] requiring prior risk assessment and due diligence, including consideration of the contractual terms that will govern the arrangement between the user and cloud service provider.

1184 PaaS is the capability to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider: Christofer Hoff "Cloud Architecture" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 17.

1185 SaaS is the capability to use the provider's applications running on a cloud infrastructure and accessible from various client services through a thin client interface such as a Web browser: Christofer Hoff "Cloud Architecture" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 17.

1186 Christofer Hoff "Cloud Architecture" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 19.

1187 See Jason Kincaid "The Sorry State of Online Privacy" (26 April 2009) *Washington Post* www.washingtonpost.com (accessed 28 April 2009). See also Electronic Privacy Information Center "In the Matter of Google, Inc. and Cloud Computing Services before the Federal Trade Commission, Complaint and Request for Injunction, Request for Investigation and Other Relief" (17 March 2009), requesting an investigation into Google's cloud computing services to determine "the adequacy of the privacy and security safeguards regarding the storage of personal information on its Cloud Computing Services".

1188 James Keller "Web-based Computing Spurs Privacy Concerns" (4 March 2009) *The Canadian Press* www.theglobeand mail.com (accessed 17 March 2009).

1189 One US law firm describes security, privacy and eDiscovery as the three biggest concerns about cloud computing: Katten Muchin Rosenman LLP and UHY Advisors FLVS Inc *Cloud Computing: Practice Safe SaaS: Don't Lose Your Head (or Data) in the Clouds* (2009).

Privacy is one of the sets of issues that arise in relation to the use of cloud computing. The type of issue that arises and its significance will depend to some extent on the type of cloud computing that is being considered.

13.77 One tool to work through the range of potential privacy issues is a Privacy Impact Assessment. Some of the potential privacy issues include:[1190]

- whether the use of cloud services by an agency holding personal information will involve an activity that is regulated by the Privacy Act (such as use or disclosure) and whether any of the exceptions apply;
- whether the use of cloud services is consistent with the organisation's privacy policy or whether people need to consent to their data being transferred to a cloud computing environment;
- assessing where the data will be located (if possible) and which privacy laws will apply;[1191]
- assessing the terms of the cloud provider's privacy statement, whether it is liable to be changed and whether it gives the cloud provider rights in relation to the cloud user's information;
- whether the cloud provider outsources any aspects of the service to other businesses, whether there is any potential for further cross-border transfers of the data and whether this impacts on the relevant privacy regulation;
- whether the data in the cloud will be held separately or comingled with the data of other cloud users;
- the limits on the scope of what the cloud provider is permitted to do with the data and whether there are any circumstances in which the service provider can access or use the data (that is, for commercial purposes such as marketing through behavioural targeting);
- whether the cloud provider can use or access transactional, relationship or metadata associated with the data being processed by the cloud service;[1192]
- the circumstances in which the data can be obtained by domestic or overseas law enforcement agencies or other third parties;
- whether the cloud service poses any risks to the security or integrity of the data being processed;
- the levels of security and encryption,[1193] including the security of data in transit, taking account of potential risks from the cloud provider, other users of the same cloud services, and cyber criminals;
- how people will be able to access and correct data about them, once it resides in a cloud environment;
- how data will be disposed of or archived once it is no longer needed;
- how the cloud user can monitor or audit the arrangement to check that the information is being held securely; and

1190 See generally Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009).

1191 See Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) 39.

1192 Robert Gellman *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* (World Privacy Forum, 2009) 21.

1193 See for example the letter by 38 researchers and academics to Google expressing concern that web-based encryption is not used as a default setting in certain aspects of its cloud based services: Electronic Information Privacy Center http://epic.org/privacy/cloudcomputing/google (accessed 17 June 2009).

- what happens to the data on termination of the cloud service, for example once the contract expires, if the cloud provider goes out of existence, if the cloud service provider unexpectedly terminates the arrangement, or if there is a merger or takeover affecting the cloud provider.

Privacy Act framework

13.78 The following Privacy Act principles and provisions are relevant to New Zealand agencies using cloud computing services.

13.79 Section 3(4) provides that where an agency (such as a cloud service provider) holds information solely for the purpose of safe custody or processing the information on behalf of another agency, and does not use or disclose the information for its own purposes, the information is deemed to be held by the agency engaging the service provider. This means that, if the cloud computing provider does not use or disclose the information for its own purposes, the agency engaging processing or custodial services remains responsible for the data under the Privacy Act, and the cloud service provider does not attract obligations under the Privacy Act. This incentivises an outsourcing agency to use a reputable service provider and ensure rigorous contractual terms to minimise the risk that the outsourcing agency will be held responsible for any breach by the service provider.

13.80 Section 10 confirms that principles 5 to 11 continue to apply to information that is held outside New Zealand by an agency (which will include information held by a cloud custodian or processor of information that does not use or disclose the information for its own purposes under section 3(4)).

13.81 Where it is necessary to give personal information to a person in connection with the provision of a service to the agency, principle 5(b) requires that everything reasonably within the power of the outsourcing agency is done to prevent unauthorised use or disclosure.[1194] One way to achieve this is through appropriate contractual arrangements.

13.82 Principle 10 contains no specific exception dealing with data processing or the outsourcing of information-handling, suggesting that where any processing or outsourcing amounts to "use" it requires the consent of those people to whom the personal information relates unless one of the other exceptions applies. However where there is no "use" of the information (such as storage services), principle 10 would not be engaged.

13.83 Likewise, principle 11 contains no specific exception dealing with processing or the outsourcing of information-handling, suggesting that where any processing or outsourcing amounts to "disclosure" to the cloud service provider, it requires the consent of those people to whom the personal information relates, unless one of the other exceptions applies. However where there is no "disclosure" of the information (such as storage services with no access rights, or secure automated processing), principle 11 would not be engaged.

1194 One issue is whether "unauthorised" in this context means (i) unauthorised by the agency engaging the service, (ii) unauthorised by the persons to whom the information relates, and thus requires consent, or (iii) unauthorised under privacy principles 10 and 11. Reference to principle 5(a)(ii) suggests that the intended interpretation is unauthorised by the agency engaging the service.

Cross-border issues

13.84 Because cloud computing will often involve data being stored in data centres offshore, it raises issues of trans-border data flows. Depending on the precise details of how an agency uses cloud computing, in cases where the provider of cloud computing services holds or processes personal information on behalf of a New Zealand agency, without using or disclosing it for the cloud provider's own purposes, section 3(4) would apply and the information held in the cloud would be deemed to be held by the New Zealand agency. The New Zealand agency would therefore remain accountable and responsible for ensuring that the privacy principles are observed.

13.85 However, where a cloud computing arrangement allows for information sharing between the user agency and the cloud service provider,[1195] this would be outside the scope of section 3(4) and the New Zealand agency would not necessarily remain accountable for the further use and disclosure of the information by the cloud service provider, except for the obligation under principle 5(b) to ensure the prevention of unauthorised use and disclosure. Except for a complaint against a user agency under principle 5(b), complaints of misuse of personal information by the cloud service provider would have to be made against that provider (which may be an offshore entity) rather than the New Zealand agency. The issues associated with trans-border data flows and options for reform are discussed in chapter 14.[1196]

13.86 It is also worth noting that where agencies and organisations that are exempt from the privacy principles[1197] use cloud services to store or process personal information, they may do so without regard to the requirements of the Privacy Act.

DEEP PACKET INSPECTION

13.87 Deep packet inspection (DPI) is a form of computer network packet filtering[1198] that can assist internet service providers (ISPs) to monitor traffic loads and manage network performance.[1199] DPI can also filter out spam and viruses. The Canadian Privacy Commissioner has noted that DPI is not a new technology, as it has been used for some time for network security purposes.[1200] What is new, however, is how DPI can potentially be deployed by ISPs in traffic management.[1201] The new potential of DPI is being hotly debated in international privacy circles because of its privacy implications. A major concern is that because DPI involves not just the inspection of traffic data (such as email addresses) but also content data (such as the content of emails),[1202] it therefore potentially allows the

1195 The information sharing would need to comply with the requirements of principle 11.

1196 See also Patrick Kershaw "Telephony the Answer for Tough Times?" (23 April 2009) *The Independent* London.

1197 Privacy Act 1993, s 2(1), definition of "agency."

1198 Including, for example, "packet sniffers."

1199 See Graham Finnie *ISP Traffic Management Technologies: The State of the Art* (Report prepared on behalf of the Canadian Radio-television and Telecommunications Commission, 2009).

1200 Office of the Privacy Commissioner of Canada *Report of Findings: Assistant Commissioner Recommends Bell Canada Inform Customers About Deep Packet Inspection* (PIPEDA Case Summary #2009-010, Ottawa, 2009) para 8.

1201 See generally See Paul Ohm "The Rise and Fall of Invasive ISP Surveillance" [2009] U Ill L Rev 1417.

1202 DPI has been described as the equivalent of opening people's mail: Saul Hansell "The Economics of Snooping on Internet Traffic" (25 March 2009) http://bits.blogs.nytimes.com (accessed 24 August 2009), attributing this comment to Tim Berners-Lee.

monitoring and collection of customers' internet activity in its entirety.[1203] Another major concern is the potential for DPI to be used for the purposes of targeted advertising.

13.88 A number of factors have given rise to the potential for DPI. These include the current use of network monitoring by ISPs to monitor network threats and viruses, improvements in network monitoring technology, the search by broadband ISPs for new sources of revenue, incentives from online advertisers, the successful adoption of behavioural targeting by other internet players such as search engines (providing a commercial model for ISPs to emulate), and the push from copyright enforcers to require ISPs to use network monitoring to control intellectual property infringements.[1204]

13.89 Several issues that we have discussed in relation to other aspects of this privacy Review are brought together in DPI including:

- the interception of electronic messages;[1205]
- the collection of internet data (discussed above); and
- behavioural targeting.[1206]

Policy responses

13.90 DPI has been the subject of review, both specifically and in the context of wider enquiries into network neutrality and the open internet, in the European Union, the United States and Canada. The European Commission initiated an investigation into British Telecom trials of ad-serving technology developed by Phorm that monitored users' web-surfing behaviour.[1207]

13.91 In the United States, 15 web-users sued NebuAd and six ISPs for violating their privacy by deploying a behavioural targeting platform that used DPI technology to monitor users' Web activity. DPI has also attracted congressional attention with hearings before the subcommittee on Communications, Technology and the Internet.[1208]

13.92 The Federal Communications Commission (FCC) has issued a notice of proposed rulemaking in relation to preserving open internet broadband industry practices.[1209] The Notice proposes the codification of a number of principles, one of which relates to transparency, requiring disclosure of internet management practices.

1203 See Electronic Privacy Information Center "Deep Packet Inspection and Privacy" http://epic.org/privacy/dpi (accessed 17 June 2009). See also Center for Democracy and Technology "The Privacy Implications of Deep Packet Inspection" (23 April 2009) Statement of Leslie Harris, President and Chief Executive of Center for Democracy and Technology before the House Subcommittee on Communications, Technology and the Internet.

1204 See generally Paul Ohm "The Rise and Fall of Invasive ISP Surveillance" [2009] U Ill L Rev 1417.

1205 See New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies (*NZLC R113, Wellington, 2010) chapter 3 and appendix A.

1206 Behavioural targeting is discussed in chapter 15.

1207 See Paul Ohm "The Rise and Fall of Invasive ISP Surveillance" (2009) U Ill L Rev, 1417 paras 17–18.

1208 Saul Hansell "Congress Begins Deep Packet Inspection of Internet Providers" (24 April 2009) http://bits.blogs.nytimes.com (accessed 8 July 2009).

1209 Federal Communications Commission "In the Matter of Preserving the Open Internet Broadband Industry Practices: Notice of Proposed Rulemaking" (22 October 2009).

13.93 The Canadian Radio-television and Telecommunications Commission (CRTC) has conducted a review of internet traffic management practices. In a submission to the review, the Canadian Privacy Commissioner compiled the following list of privacy questions raised by DPI:[1210]

- What are the appropriate uses of DPI?
- When should DPI be activated and under what authority?
- What information management processes and controls should be used by organisations deploying DPI technology, or third parties with access to this information?
- What should be required in relation to:
  - informing the customer about the use of DPI;
  - customer choices regarding use of DPI for security; and
  - customer choices regarding use of DPI for selling profiling data to third parties?
- What information that is potentially examinable by DPI constitutes personal information and is, therefore, subject to the protections of privacy legislation?
- Should consideration be given to the appropriateness of underlying design decisions as the exploitation of weaknesses gives rise to the need for DPI?

13.94 While noting that privacy concerns relate to the *potential* use of technologies used for internet traffic management practices rather than their current use, the CRTC concluded that it would be appropriate to impose a higher standard than required under PIPEDA to ensure a higher degree of privacy protection for telecommunications customers. The Commission has directed that:[1211]

- ISPs are not to use personal information collected for the purposes of traffic management for other purposes, and are not to disclose such information; and
- ISPs are to disclose internet traffic management practices to customers clearly and prominently on their websites.

13.95 The Canadian Privacy Commissioner has devoted a section of the Office's website to issues associated with DPI[1212] and has investigated a complaint about the DPI practices of Bell Canada.[1213] The Privacy Commissioner rejected complaints that Bell was collecting personal information about customers without their consent and that Bell was gathering more information than it needed to manage its network. However the Privacy Commissioner did require Bell to change its service agreements, and the Frequently Asked Questions section of its website, to notify customers that it collects and retains personal information through use of its DPI technology.[1214]

1210 Office of the Privacy Commissioner of Canada "Review of the Internet Traffic Management Practices of Internet Service Providers" (Submission to the Canadian Radio-television and Telecommunications Commission, 2009).

1211 Canadian Radio-television and Telecommunications Commission "Review of the Internet Traffic Management Practices of Internet Service Providers" www.crtc.gc.ca (accessed 20 November 2009).

1212 Office of the Privacy Commissioner of Canada *Deep Packet Inspection: A Collection of Essays from Industry Experts* http://dpi.priv.gc.ca (accessed 8 December 2009).

1213 Office of the Privacy Commissioner of Canada *Report of Findings: Assistant Commissioner Recommends Bell Canada Inform Customers About Deep Packet Inspection* (PIPEDA Case Summary #2009-010, Ottawa, 2009).

1214 Office of the Privacy Commissioner of Canada *Report of Findings: Assistant Commissioner Recommends Bell Canada Inform Customers About Deep Packet Inspection* (PIPEDA Case Summary #2009-010, Ottawa, 2009).

New Zealand regulatory framework

13.96 Deep packet inspection is potentially regulated in New Zealand by interception offences in the Crimes Act.[1215] Under the civil law, the collection of telecommunications information is governed by the Telecommunications Information Privacy Code 2003 which modifies the application of the privacy principles in relation to telecommunications.

Telecommunications Information Privacy Code

13.97 "Telecommunication" is given the same meaning as under the Telecommunications Act 2001:[1216]

> The conveyance by electromagnetic means from one device to another of any encrypted or non-encrypted sign, signal, impulse, writing, image, sound, instruction, information, or intelligence of any nature, whether for the information of any person using the device or not.

13.98 The Code applies to information about an identifiable individual that is:[1217]

- subscriber information (personal information about a subscriber which is obtained by an agency at the time the subscriber subscribes or during the term of the contractual relationship);
- traffic information (call associated data[1218] and any other dialling or signalling information generated as the result of making a telecommunication); and
- the content of a telecommunication.

The Code extends to ISPs.[1219]

13.99 The use of DPI by ISPs is likely to involve the collection of telecommunications directly from their customers but because of the range of exceptions to the notice requirement (such as that there will be no prejudice to the customer's interests, or notification is not practicable, or the information will not be used in a form

---

1215 Crimes Act 1961, s 216B(1), although s 216B(5) contains an exception for employees of internet service providers carrying out network maintenance services.

1216 Telecommunications Act 2001, s 5.

1217 Telecommunications Information Privacy Code 2003, cl 4(1).

1218 Call associated data is defined in the Telecommunications Information Privacy Code 2003, cl 3 as follows:

(a) dialling or signalling information

(i) generated as a result of the making of the telecommunication (whether or not the telecommunication is received successfully); and

(ii) that identifies the origin, direction, destination, or termination of the telecommunication; and

(b) without limiting the generality of paragraph (a), includes any of the following information:

(i) the number from which the telecommunication originates:

(ii) the number to which the telecommunication is sent:

(iii) if the telecommunication is diverted from one number to another number, those numbers:

(iv) the time at which the telecommunication is sent:

(v) the duration of the telecommunication:

(vi) if the telecommunication is generated from a mobile telephone, the point at which the telecommunication first enters a network; but

(c) does not include the content of the telecommunication.

1219 Telecommunications Information Privacy Code 2003, cl 4(2).

that identifies the customer), there may be an issue as to whether customers would always get notice about DPI. There is also a specific exception to notice where the collection is for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity.[1220]

13.100 Where the telecommunications information of non-customers (such as email recipients) is collected incidentally through DPI of the internet activity of ISP customers, there is no particular notification requirement. Rule 2 requires telecommunications information to be collected directly from the individual concerned; however, this is not required if not reasonably practicable.[1221] There is also an express exception for the collection of traffic information.[1222]

13.101 The use and disclosure of telecommunications information for a purpose other than the purpose for which it was collected is limited under rules 10 and 11. However, the use and disclosure of information collected through DPI for an intended purpose such as behavioural targeting is not expressly restricted.

13.102 The Code expressly permits ISPs to monitor call associated data where necessary to investigate an action that may threaten network security or integrity (subject to section 107 of the Telecommunications Act which prohibits the use of telephone analysers, although there is an exception for maintenance of the network) but this does not extend to content data.[1223]

13.103 Depending on its extent, the collection of personal information using DPI may be unlawful (and, indeed, criminal[1224]) or unfair, or may intrude to an unreasonable extent into the personal affairs of an individual, which would make it in breach of rule 4.

LOCATION TECHNOLOGIES

13.104 In *Privacy: Concepts and Issues*, we outlined developments in relation to location technologies.[1225] The global positioning system (GPS) transmits satellite signals to a receiver, making it possible to determine where a person is at any given time, or where a person has been, by accessing location data. Location data is also generated by cellphones, payment and entry systems such as transit swipe cards (for example, Wellington's Snapper cards), electronic tolling devices and electronic swipe cards for doors. Companies continue to develop location-based services for the internet. For example, Google Latitude allows users to share their cellphone location with friends via the internet or smart phone.[1226]

13.105 In the report for stage 3 of our Review we recommended the creation of a new criminal offence where someone uses a tracking device to determine someone else's location without consent, and we gave examples of scenarios that the

1220 Telecommunications Information Privacy Code 2003, cl 5, rule 3(4)(b)(iii).

1221 Telecommunications Information Privacy Code 2003, cl 5, rule 2((2)(f).

1222 Telecommunications Information Privacy Code 2003, cl 5, rule 2((2)(h).

1223 Telecommunications Information Privacy Code 2003, cl 5, rule 4.

1224 For example if it involves the "interception of a private communication" that does not fall within the service provider exception: Crimes Act 1961, s 216B(5).

1225 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.81–6.89.

1226 See, eg, Ian Paul "Google Latitude Services Lets You Track Your Friends: How It Works" (5 February 2009) *PC World*; David Coursey "Spy on Your Workers with Google Latitude" (5 February 2009) *PC World* www.pcworld.com (accessed 24 February 2010).

offence is intended to cover.[1227] The proposed offence would cover the active use of a device to produce location data without the consent of the target of the surveillance and would prohibit the disclosure of information thus obtained, but would not otherwise prohibit the handling and use of location data.

13.106 The development of location technologies has led to concerns about preserving spatial (or "locational") privacy. The Electronic Frontier Foundation has called for location tracking systems to be built with privacy as a central component of their design. It is possible to create systems that do not in fact collect locational data, whilst still delivering the service they are designed to deliver.[1228]

13.107 The European Union Directive on Privacy and Electronic Communications deals explicitly with location data in the electronic communications sector.[1229] The Directive prohibits the processing of location data that has not been anonymised without the consent of the user of the service. It also requires service providers to inform users, before obtaining their consent, of the type of location data to be processed, the purpose and duration of the proposed processing, and whether the data will be transmitted to a third party. Users must be given the opportunity to withdraw their consent at any time. Processing of the data must be restricted to that which is necessary for the purpose of providing the service.[1230]

RADIO FREQUENCY IDENTIFICATION

13.108 In *Privacy: Concepts and Issues*, we outlined developments in relation to radio frequency identification (RFID),[1231] which raises some similar issues to location technologies. RFID technology can be used for a variety of purposes. It was first developed as a mechanism for inventory control to replace barcodes. Current uses of RFID in New Zealand include office swipe cards, the new biometric passport and microchipping of dogs. There are concerns about its potential to track people by the tagged objects they carry or potentially by means of a chip implanted under the skin.[1232] Privacy concerns about RFID also arise from the ability for RFID data to be aggregated with other information so as to create detailed profiles about consumers, and the ability to clone RFID chips.

1227 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, Wellington, 2010) paras 3.46–3.54, recommendation 8.

1228 Andrew J Blumberg and Peter Eckersley *On Locational Privacy, and How to Avoid Losing it Forever* (Electronic Frontier Foundation, San Francisco, 2009).

1229 European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201.

1230 European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201, cited in Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 9.88.

1231 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.71–6.80. See also New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2009) paras 10.72–10.74.

1232 See Ian Kerr "The Internet of People? Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification" in Ian Kerr, Valerie Steeves and Carole Lucock (eds) *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, New York, 2009).

13.109 In the United States, a number of states have actively considered RFID legislation and in a few states, legislation has been passed.[1233] The European Commission has adopted a Recommendation that provides guidance on how to operate RFID applications in compliance with privacy and data protection principles and industry has welcomed the framework.[1234] A central theme is that privacy and information security features should be built into RFID applications before their widespread use.[1235] The OECD has also issued policy guidance on RFID that covers privacy issues such as transparency and notice, and privacy and security risk assessment.[1236]

13.110 In the UK the Information Commissioner has published information about RFID tags and data protection.[1237] The Office of the Privacy Commissioner of Canada has produced a fact sheet on RFID technology[1238] and a consultation paper on RFID in the workplace.[1239] The Information and Privacy Commissioner of Ontario has issued a set of best practice guidelines in collaboration with industry and stakeholders.[1240] As we noted in *Privacy: Concepts and Issues*, an industry code of practice has been developed in New Zealand.[1241]

BIOMETRICS

13.111 In *Privacy: Concepts and Issues*, we discussed certain technologies of the body including biometrics, genetic technology and brain scanning.[1242] Biometric technologies include finger and iris scanning, and facial, voice and gait recognition. They are used to identify individuals or to verify their identity by means of their physical features. Some can be used covertly and at a distance, and in addition to their use in identification they may give clues as to what a person is thinking or feeling.

13.112 Biometrics give rise to particular privacy concerns due to their links with a person's bodily identity and sense of personhood. Privacy concerns about the use of biometrics include that the technology makes it easier to monitor people and link information about them and that biometrics may reveal sensitive information such as information about a person's health, emotional state or ethnicity. There are also concerns about security and accuracy.

1233 Julie Manning Magid, Mohan V Tatikonda and Philip L Cochran "Radio Frequency Identification and Privacy Law: An Integrative Approach" (2009) 1 Am Bus LJ 19–22. See also Laura Hildner "Defusing the Threat of RFID: Protecting Consumer Privacy through Technology-Specific Legislation at the State Level" (2006) 41 Harv CR-CL L Rev 133.

1234 Paul Mueller "EC Sets Out Privacy Requirements for Smart RFID Tags" (13 May 2009) *IDG News Service* http://computerworld.co.nz (accessed 19 May 2009).

1235 European Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (12 May 2009) C(2009)3200.

1236 OECD Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development *OECD Policy Guidance on Radio Frequency Identification* (Paris, 2008). See Blair Stewart, Assistant Privacy Commissioner "Tracking down good privacy practices for RFID" (Presentation to New Zealand RFID Pathfinder Group, Auckland, 9 July 2009).

1237 Information Commissioner's Office (UK) *Data Protection Technical Guidance – Radio Frequency Identification* (2006) www.ico.gov.uk (accessed 8 December 2009).

1238 Office of the Privacy Commissioner of Canada *RFID Technology* www.privcom.gc.ca (accessed 9 December 2009).

1239 Office of the Privacy Commissioner of Canada *Radio Frequency Identification in the Workplace: Recommendations for Good Practices – a Consultation Paper* (Ottawa, 2008).

1240 Information and Privacy Commissioner of Ontario *Privacy Guidelines for RFID Information Systems* (Toronto, 2006).

1241 GS1 New Zealand *EPC/RFID Consumer Code of Practice* www.gs1nz.org (accessed 18 January 2010); New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.73.

1242 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.90–6.95.

13.113 The Irish Council for Bioethics has released a report raising concerns about how personal biometric information is collected and stored and whether there are sufficient controls on who can access it. The Council recommends that any use of biometrics should be proportional to the risk sought to be addressed and that a detailed justification should be provided as to why using biometrics advances the public good. There should be openness and transparency around the use of biometrics. Furthermore, information collected should not be shared without cause, should not be held for longer than necessary, and should be deleted when no longer needed.[1243]

13.114 In Australia, the Biometrics Institute developed its own Privacy Code, which was approved by the Australian Privacy Commissioner in 2006 and applies to members of the Institute. The Code modifies the Australian Privacy Act's principles for biometrics, and also adds several supplementary principles, covering protection of biometric information, individuals' ability to control the use of biometric information about them and accountability of members.[1244]

13.115 The New Zealand Privacy Commissioner has noted that a code of practice is one possible avenue to respond to the issues posed by biometrics, but that this is a resource-intensive option.[1245] The New Zealand Government has released *Guiding Principles for the Use of Biometric Technologies for Government Agencies*.[1246] The new Immigration Act 2009 makes provision for the collection of biometric information by specified immigration officials, and imposes a requirement that the information be dealt with in accordance with the Privacy Act.[1247] Moreover the provisions limit the purposes for which biometric information can be collected.[1248] In respect of the collection and use of biometric information by immigration officials, the Department of Immigration is required to carry out a privacy impact assessment in order to identify the inroads into an individual's privacy, and to consider ways to mitigate any potential harms that are identified.[1249] In doing so, the Department must consult with the Privacy Commissioner.

13.116 Noting that agencies are increasingly using biometric information as identifiers, the ALRC has recommended an amendment to the identifier principle (the equivalent of New Zealand's principle 12) to make it clear that the principle covers the use of biometric information for identification purposes.[1250] The Commission recommended that an "identifier" should include "biometric information that is collected for the purpose of automated biometric identification or verification that (a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or (b) is determined to be an identifier

1243 Irish Council for Bioethics *Biometrics: Enhancing Security or Invading Privacy?* (Dublin, 2009).

1244 Office of the Privacy Commissioner (Cth) "Approval of the Biometrics Institute Privacy Code" (19 July 2006).

1245 Marie Shroff, Privacy Commissioner "Trans Tasman Standardisation for Biometrics" (Address to the Biometrics Institute Trans Tasman Standardisation for Biometrics Conference, Wellington, 1 October 2004).

1246 Cross Government Biometrics Group *Guiding Principles for the Use of Biometric Technologies for Government Agencies* (Wellington, 2009).

1247 Immigration Act 2009, s 31.

1248 Immigration Act 2009, s 30.

1249 Immigration Act 2009, s 32.

1250 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 30.48–30.58, recommendation 30-3. The Australian Law Reform Commission also recommended that biometric information that is collected for the purpose of automated biometric verification or identification, as well as biometric template information, be treated as "sensitive information" for purposes of the Australian Privacy Act: Recommendation 6-4.

by the Privacy Commissioner."[1251] In its response, the Australian Government rejected this information, on the basis that the "identifier" principle is not appropriate for addressing the harm identified by the ALRC.[1252]

PRIVACY-ENHANCING TECHNOLOGIES

13.117 In *Privacy: Concepts and Issues*, we discussed different types of privacy-enhancing technologies (PETs).[1253] PETs encompass both tools that individuals can use to protect their privacy online (such as encryption and data anonymisation)[1254] and tools that can be used by organisations to minimise the intrusiveness of their systems on the privacy of members of the public. We noted three roles that PETs can play in privacy policy:[1255]

- they can compliment other regulatory approaches as part of the privacy protection "toolbox";
- the use of specified PETs in particular products or services could be mandated by regulation or legislation; or
- they can be used as alternatives to regulation.

We also noted that government can encourage the use of PETs through taking the lead by mandating their adoption by government agencies and other public entities.

13.118 The House of Lords Constitution Committee has recently endorsed the use of PETs to ensure "privacy by design": that is, ensuring that systems are designed to incorporate privacy protections from the outset.[1256] The committee recommended that the UK Government review its procurement processes so as to incorporate design solutions that include privacy-enhancing technologies in new or planned data gathering and processing systems.[1257] In Canada, the Information and Privacy Commissioner of Ontario has also been very active in promoting "privacy by design".[1258]

13.119 Privacy impact assessments (PIAs) are one tool that could help to identify where PETs could be implemented in the design of new initiatives, and the Privacy Commissioner has produced a *Privacy Impact Assessment Handbook*.[1259] The House of Lords Constitution Committee has recommended that the UK Government amend the provisions of the Data Protection Act 1998 so as to make

1251 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 30.48–30.58 and 30.146, recommendation 30-3.

1252 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 74.

1253 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 151–156.

1254 See also new developments such as the Vanish programme that makes data unreadable after a certain time period: Mark Harris "How You Can Self-Destruct Your Messages" (16 August 2009) *Times OnLine* http://technology.timesonline.co.uk (accessed 20 August 2009); John Markoff "New Technology to Make Digital Data Self-Destruct" (21 July 2009) *The New York Times* www.nytimes.com (accessed 29 July 2009).

1255 Colin J Bennett and Charles D Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge (Mass), 2006) 198–202, cited in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Welington, 2008) 155.

1256 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009).

1257 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009) para 349.

1258 See, for example, Ann Cavoukian, Information and Privacy Commissioner of Ontario *Privacy by Design: The 7 Foundational Principles* (Toronto, 2009).

1259 Office of the Privacy Commissioner *Privacy Impact Assessment Handbook* (Wellington, 2007).

it mandatory for government departments to produce an independent, publicly available, full and detailed PIA prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing.[1260]

13.120 The ALRC has recommended that the Privacy Commissioner should have the power to direct a public agency to produce a PIA in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[1261] If an agency failed to comply, the Privacy Commissioner would be required to report to the responsible Minister.[1262] The Australian Government accepted this recommendation.[1263] The ALRC also recommended that the Privacy Commissioner produce guidelines in relation to PIAs,[1264] and that this new function be reviewed in five years' time to assess whether it should be extended to private sector organisations.[1265] This recommendation was also supported by the Australian Government.[1266]

13.121 The Privacy Commissioner's function to promote an understanding of the privacy principles by education and publicity[1267] is broad enough to enable the Privacy Commissioner to undertake educational programmes about PETs. The ALRC has recommended that in exercising its research and monitoring functions, the Australian Privacy Commissioner's Office should explicitly consider technologies that can be deployed in a privacy-enhancing way; and that the Office should develop and publish education materials for individuals and agencies about specific PETs and privacy-enhancing ways in which technologies can be deployed.[1268] Both recommendations were accepted by the Australian Government in its response.[1269]

13.122 In the United Kingdom, the Information Commissioner has commissioned research to develop a compelling and understandable business case for investing in proactive privacy protections. This arose from an earlier report that identified the absence of an articulated business case for spending money on privacy-friendly systems as a barrier to more proactive privacy protection.[1270]

1260 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009) para 307. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these PIAs.

1261 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-4(a). The Commission preferred this option to the alternative option of mandatory Privacy Impact Assessments as is the case in Canada: para 47.61.

1262 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-4(b).

1263 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 86.

1264 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-5.

1265 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 47-5.

1266 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 87.

1267 Privacy Act 1993, s 13(1)(a).

1268 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendations 10-1 and 10-2.

1269 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 30.

1270 Information Commissioner's Office (UK) *The business case for investing in proactive privacy protection* (London, 2009).

Q158 Do you have any comments about the role of privacy-enhancing technologies in government or the private sector, and how their use could be encouraged?

Q159 Should consideration be given to empowering the Privacy Commissioner to direct public or private sector agencies to produce Privacy Impact Assessments for new projects that may have a significant impact on the handling of personal information?

CONCLUSION

13.123 In this chapter we have outlined technological practices that give rise to particular privacy concerns and have asked for views about the issues raised. As noted above, the Privacy Commissioner has a specific function to research and monitor developments in data processing and computer technology, and to ensure that any adverse privacy effects of such developments are minimised.[1271] We think that this function should probably be broadened and updated so that instead of referring to "data processing and computer technology" it refers to a broader range of technological developments.[1272] We wonder whether the Privacy Commissioner's responsibility to *ensure* the minimisation of privacy effects remains realistic and we suggest that this aspect may need to be revisited. We also note that the Australian Privacy Act provides the Australian Privacy Commissioner with an additional function to monitor and report on the adequacy of equipment and user safeguards.[1273]

13.124 We invite submissions relating to the functions of the Privacy Commissioner in relation to technological developments, and relating to the topics discussed in this chapter.

Q160 Do you have any comments about the privacy issues associated with the technologies discussed in this chapter? Is any particular law reform or regulatory response required in relation to any or all of these technologies? Should consideration be given to codes of practice or Privacy Commissioner guidelines in relation to any particular technology?

Q161 Do technologies not discussed in this chapter give rise to important privacy issues that require examination?

1271 Privacy Act 1993, s 13(1)(n).

1272 The Australian Law Reform Commission has recommended deleting the word "computer" from the comparable function of the Australian Privacy Commissioner in the Privacy Act 1988 (Cth), s 27(1)(c): Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-1.

1273 Privacy Act 1988 (Cth), s 27(1)(q).

Chapter 14

Trans-border data flows

14.1 Technological innovation and globalisation have facilitated a surge in trans-border flows of information. The internet, in particular, has enabled information to be moved around the world almost instantly.[1274] These developments have major implications for the protection of informational privacy, and create significant challenges for national information privacy laws like the Privacy Act 1993.

14.2 This chapter looks at the international context and the current legal position in New Zealand with regard to the transfer of personal information across borders. It considers options for law reform to better provide for the protection of privacy in relation to trans-border data flows, and then looks at specific issues relating to cross-border cooperation for the enforcement of privacy laws, and steps that might need to be taken to implement the APEC Privacy Framework.

BACKGROUND[1275]

14.3 Trans-border data flows are increasingly prevalent in modern commerce and government and individuals may frequently not even realise that their information is being sent overseas. Some examples of trans-border data flows are:[1276]

- Businesses and governments are increasingly outsourcing activities, including the processing of personal information about their customers and citizens.
- Even where a transaction ostensibly takes place within New Zealand, information may often be routed through overseas computer servers. This is often the case with, for example, email and credit card details used to make online purchases.
- Technologies such as search engines, cloud computing and voice over internet protocol can all involve personal information being sent overseas.

1274 New Zealand Law Commission *Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) 158.

1275 We have previously discussed some of these issues in New Zealand Law Commission *Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) chapter 7.

1276 Examples taken from Marie Shroff, Privacy Commissioner "Privacy and Sovereignty: Data fight or flight?" (Address to GOVIS 2007 – Innovation in ICT, Wellington, 10 May 2007) 2–4; Jennifer Stoddart, Privacy Commissioner of Canada "Privacy Protection in a World of Trans-border Data Flows" (Paper presented to Working Party on Information Security and Privacy (OECD), Paris, 3 October 2005); David Loukidelis, Information and Privacy Commissioner for British Columbia "Trans-border Data Flows & Privacy – An Update on Work in Progress" (Address to 7th Annual Privacy & Security Conference, Victoria (BC) 10 February 2006).

- A mirror image of all New Zealanders' passport data is stored in Australia to facilitate the advanced passenger processing system. Immigration New Zealand accesses passports information through Sydney.
- Motivated by concerns about terrorism and national security, governments are demanding more information about people entering their countries. Airline passenger information about all international air travellers, including ticketing and bookings, is transmitted electronically to Atlanta. The US Department of Homeland Security has sought access to this global database for anti-terrorism purposes.

14.4 Paul Swartz has noted some important recent changes in the way international data transfers are occurring. These are:[1277]

- A change in scale. Formerly, companies generally worked with discrete, localised data sets, data processing systems were generally nationally-based and an international data flow was an exceptional event. Now, trans-border data flows are continuous and multipoint, and there has been massive growth in the complexity and volume of these flows.
- A change in processing. Formerly, an international data flow occurred at a predictable moment and into a database controlled by a single entity. In contrast, data transmissions now occur as part of a networked series of processes, and increasingly occur on demand. New technologies allow significant flexibility as to how data flows occur. For example, computing activities can be shifted from one country to another depending on load capacity, time of day and a range of other factors.
- A change in management. Corporate data processing is becoming professionalised and businesses are now investing more resources in this area.

14.5 It will be evident that trans-border data flows can entail significant opportunities for agencies, but that there are corresponding privacy risks. Some countries where personal information about New Zealanders is sent may not have laws in place to protect privacy to the standard that New Zealanders expect. This could result in personal information being exposed. New Zealanders may also not be able to exercise the same rights to seek redress as they can in New Zealand. As the Organisation for Economic Co-operation and Development (OECD) has noted:[1278]

> When personal information moves across borders it may put at increased risk the ability of individuals to exercise privacy rights to protect themselves from the unlawful use or disclosure of that information. At the same time, privacy enforcement authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities of organisations outside their borders.

1277 Paul M Schwartz "Managing Global Data Privacy: Cross-border Information Flows in a Networked Environment" (Paper to OECD Working Party on Information Security and Privacy, Paris, 12–13 October 2009).

1278 Organisation for Economic Co-operation and Development *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007) 4.

14.6 The State Services Commission, in guidance for agencies on off-shoring, has usefully outlined the potential privacy risks that can arise from sending personal information overseas for processing. They include:[1279]

- non-compliance with Privacy Act;
- unauthorised release of personal information;
- inability to provide data subjects with access to their personal information;
- inability to cooperate with the Privacy Commissioner over complaints of interference with privacy;
- inability of the Privacy Commissioner to investigate or enforce against offshore offenders;
- inability to guarantee the protection of personal information in countries that do not have privacy/data protection laws;
- foreign laws that conflict with the Privacy Act or offer less protection for the privacy of personal information;
- a particular country's laws that may enable its government to gain access to New Zealanders' personal information without the knowledge or authorisation of the New Zealand government;
- overseas judicial decisions that might require disclosure of New Zealand personal information held offshore, or allow the commercial use of that information;
- problems with recovery and/or secure disposal of personal information at the termination of an outsourcing relationship; and
- loss of trust in government if government agencies outsource processing of personal information and a data breach occurs

14.7 The challenge, then, is to allow trans-border data flows to occur whilst also protecting privacy. A range of international and regional instruments have been developed in pursuit of the twin goals of facilitating free flows of information across borders and protecting privacy. Each seeks to establish consistent rules among countries so that inconsistent national laws do not impede trans-border data flows and economic development.[1280]

INTERNATIONAL CONTEXT

14.8 A number of international privacy instruments have been developed since the 1980s, with the aim of setting privacy standards to facilitate consistent domestic laws. As yet, however, no international privacy treaty exists, although it is sometimes suggested.[1281] The ultimate goal appears to be that all countries will have similar privacy standards, so barriers to trans-border data flows will no longer be necessary. In the interim, international instruments aim to set similar standards for members, so that information flows between member countries can occur unimpeded.

1279 State Services Commission *Government Use of Offshore Information and Communication Technologies (ICT) Service Providers: Advice on Risk Management* (Wellington, 2009) 6–7, 14–15 and 26–27.

1280 Blair Stewart, Assistant Privacy Commissioner "The Economics of Data Privacy: Should we place a dollar value on personal autonomy and dignity?" (Paper to 26th International Conference of Privacy and Data Protection Commissioners, Wroclaw (Poland), 14–16 September 2004) 3.

1281 The International Law Commission has added the topic "Protection of personal data in the trans-border flow of information" on its long term work programme: UNGA "Report of the International Law Commission" (58th Session, 1 May–9 June and 3 July–11 August 2006) A/61/10. Work on this does not appear to be progressing quickly.

14.9 The international privacy instruments that are most relevant to New Zealand are those of the OECD, Asia-Pacific Economic Cooperation (APEC), European Union (EU) and United Nations (UN). This section outlines these international instruments as they relate to trans-border data flows, in chronological order. Particular potential reforms arising from them will be discussed in more detail later in the chapter.

OECD Guidelines

14.10 The OECD Guidelines,[1282] issued in 1980, form the basis for many countries' privacy legislation, including New Zealand's Privacy Act. The Guidelines aimed to promote trans-border data flows through consistent national legislation. Thus, the recitals recognise:

> That although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information … That automatic processing and trans-border flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices … That trans-border flows of personal data contribute to economic and social development … That domestic legislation concerning privacy protection and trans-border flows of personal data may hinder such trans-border flows.

14.11 In relation to trans-border data flows, the Guidelines provide that:

> 15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
>
> 16. Member countries should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a Member country, are uninterrupted and secure.
>
> 17. A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
>
> 18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans-border flows of personal data that would exceed requirements for such protection.

Beyond this, however, they do not prescribe a particular approach that member countries themselves should take in their legislation to deal with trans-border data flows.

1282 *Recommendation of the Council of the Organisation for Economic Cooperation and Development concerning Guidelines governing the protection of privacy and trans-border flows of personal data* (1980).

Council of Europe

14.12 The Council of Europe's Convention No 108 was adopted in 1981.[1283] It has been influential, underlying subsequent Council of Europe recommendations and the 1995 EU Directive, discussed below. The Convention may be acceded to by countries outside Europe by a specific procedure.

14.13 Article 12 relates to trans-border flows of personal data, stating:

> 1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
>
> 2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation trans-border flows of personal data going to the territory of another Party.
>
> 3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
>
> (a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
>
> (b) when the transfer is made from its territory to the territory of a non-contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

14.14 Protocol 181 to the Convention was adopted in 2001 and deals with cross-border data flows.[1284] Its approach is based on the EU Directive. Article 2 provides that parties may only allow transfers of personal data to non-parties if the receiving state or organisation ensures an adequate level of protection for the intended data transfer.

United Nations guidelines

14.15 The UN produced privacy guidelines in 1990.[1285] They have not been very influential and do not add much to OECD and Council of Europe work. Principle 9 is about trans-border data flows and provides:

> When the legislation of two or more countries concerned by a trans-border data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

1283 Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data (28 January 1981) CETS 108.

1284 Additional Protocol to the Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows (8 November 2001) CETS 181.

1285 UNGA Resolution 44/132 "Guidelines for the regulation of computerised personal data files" (1989) A/44/49.

EU Directive[1286]

14.16 The EU Directive[1287] requires EU member countries to prohibit the transfer of personal data to countries that do not have privacy laws meeting the Directive's standards.[1288] Three European Economic Area states (Iceland, Liechtenstein and Norway) that are not EU members are also bound by the directive. Article 25 provides:

> 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.
>
> …
>
> 4. Where the Commission finds … that a country does not ensure an adequate level of protection … Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
>
> …
>
> 6. The Commission may find … 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 … for the protection of the private lives and basic freedoms and rights of individuals.

14.17 Data may be exported freely to countries that have been judged to provide an adequate level of protection under article 25(6), without the need for any further controls. This is generally referred to as a finding of "EU adequacy". Countries that currently have this status are Argentina, Canada, Switzerland, the US Safe Harbour scheme and Transfer of Air Passenger Name Record Data, Guernsey, the Isle of Man and Jersey.[1289]

14.18 In addition, Article 26 provides for exceptions where transfers may be made even where the third country has not ensured an adequate level of protection. The exception applies where:

- there is unambiguous consent from the data subject;

1286 See also discussion of the Directive in New Zealand Law Commission *Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) paras 7.43–7.64.

1287 European Parliament and Council Directive 95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281.

1288 See generally G Greenleaf "Global Protection of Privacy in Cyberspace – 3. The EU Directive's data export requirements" (Paper to Science & Technology Law Center 1998 Internet Law Symposium, Taipei, 23–24 June 1998).

1289 European Commission Directorate-General for Justice, Freedom and Security "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries" http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm (accessed 5 February 2010).

- the transfer is necessary for the performance, implementation or conclusion of certain contractual transaction;
- the transfer is in the public interest or the vital interests of the data subject; or
- the transfer is made from a public register.

Member states may also transfer data where a contract contains adequate privacy safeguards.

14.19 So, the fact that a country has not achieved adequacy does not mean that no information may be sent from the EU to that country. However, an adequacy finding simplifies matters considerably. Submitters to the Australian Law Reform Commission's (ALRC) review of the Australian Privacy Act noted that, although not essential for businesses to trade with EU countries, an adequacy finding would help streamline trade between Australian businesses and Europe.[1290]

14.20 Another aspect of the EU data protection system is the system of binding corporate rules (BCRs), which are similar to APEC cross-border privacy rules, discussed below. BCRs were developed for use by a multinational organisation or group of companies as a mechanism for transferring personal data across borders throughout the organisation under a single standard. BCRs must be approved by every European data protection authority in whose jurisdiction the organisation (or member of the group) will rely on them.[1291] Standardised processes and guidance to business have been developed, and data protection authorities are taking a cooperative approach, so that the system is now beginning to work well.

APEC

14.21 The APEC Privacy Framework ("the Framework") was endorsed by APEC Ministers in 2004.[1292] It aims to promote electronic commerce by harmonising members' data protection laws and facilitating information flows through the region. APEC members are not obliged to implement the Framework domestically in any particular way.

14.22 The Framework establishes a set of ten privacy principles. Principle 9 is the most relevant to trans-border data flows. It provides that a personal information controller:

> Should be accountable for complying with measures that give effect to the Principles… When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.

1290 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 31.31.

1291 See, for example, "The effect of binding corporate rules on overseas transfers of personal data" www.out-law.com (accessed 22 December 2009).

1292 Asia-Pacific Economic Cooperation "APEC Privacy Framework" (16th APEC Ministerial Meeting, Santiago, 17–18 November 2004) 2004/AMM/0114rev1.

14.23 Another important feature of the Framework is that it allows organisations to develop cross-border privacy rules that apply across the APEC region. The Framework provides:[1293]

> Member Economies will endeavour to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.

In order to give effect to such rules, member economies are instructed to develop frameworks or mechanisms for mutual recognition of cross-border privacy rules between economies. Such frameworks should "facilitate responsible and accountable cross-border data transfers without creating unnecessary barriers to cross-border information flows."[1294]

14.24 The idea of a cross-border privacy rules system has been described as follows:[1295]

> The aim of an APEC system to protect personal information is to encourage organizations to develop their own internal business rules on privacy procedures governing the movement of personal information across borders. These business rules will apply to an organization's operations and business units throughout the APEC region. Organizations would then be held accountable for complying with their rules by an appropriate authority, such as a regulator. It is these rules developed by organizations that are known as the APEC cross-border privacy rules.

14.25 In 2007, the APEC Ministerial Meeting launched the APEC Data Privacy Pathfinder initiative ("the Pathfinder").[1296] Its purpose is to enable member countries to work together on implementing the Framework, focusing on developing a system of cross-border privacy rules. Member countries cluster into groups in order to "pilot the implementation of cooperative initiatives prior to their adoption by all APEC members." There are currently nine Pathfinder projects working on developing aspects of the cross-border privacy rules system.[1297] We understand that so far it has proved difficult to translate the idea of cross-border privacy rules into reality. However, the Pathfinder has resulted in the successful completion of the Cross-border Enforcement Cooperation Agreement, which complements the OECD Recommendation discussed below.

1293 Asia-Pacific Economic Cooperation "APEC Privacy Framework" (16th APEC Ministerial Meeting, Santiago, 17–18 November 2004) 2004/AMM/0114rev1, para 46.

1294 Asia-Pacific Economic Cooperation "APEC Privacy Framework" (16th APEC Ministerial Meeting, Santiago, 17–18 November 2004) 2004/AMM/0114rev1, paras 47 and 48.

1295 Asia-Pacific Economic Cooperation "Project 8 – Scope & Governance of a Cross-Border Privacy Rules System" (Item for 20th Electronic Commerce Steering Group Meeting (DPS), Singapore, 28 July 2009) 2009/SOM2/ECSG/DPS/009.

1296 Asia-Pacific Economic Cooperation "APEC Data Privacy Pathfinder" (Item for Concluding Senior Officials' Meeting, Sydney, 2–3 September 2007) 2007/CSOM/019.

1297 Asia-Pacific Economic Cooperation "APEC Data Privacy Pathfinder Projects Implementation Work Plan" (Item for 17th Electronic Commerce Steering Group Meeting, Lima, 24 February 2008) 2008/SOM1/ECSG/024.

OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy

14.26 The OECD's work on enforcement cooperation has been driven by increasing concerns about the privacy risks associated with the changing character and growing volume of cross-border data flows. Closer cooperation among privacy law enforcement authorities (such as New Zealand's Privacy Commissioner) is seen as a means of better safeguarding personal data. The OECD recommends:

> That Member countries co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:
>
> (a) Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.
>
> (b) Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.
>
> (c) Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.
>
> (d) Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

We discuss the Recommendation, and its implementation in New Zealand, in more detail later in this chapter.

International standards

14.27 A number of organisations are working on developing international privacy standards. The International Organisation for Standardisation has developed an information security standard (ISO 17799) and is also working on developing privacy standards. The International Conference of Data Protection and Privacy Commissioners passed a resolution in 2007 endorsing "the development of effective and universally accepted international privacy standards." The resolution noted that standards have an important role to play, alongside legislation, and that they can be a way of translating "legal requirements into concrete practices."[1298] The Conference continues to promote international standards.[1299]

CURRENT SITUATION IN NEW ZEALAND

Privacy Act

14.28 Currently, the main provision in the Act that deals with trans-border data flows is section 10, which provides:

> **Application of principles to information held overseas**
>
> (1) For the purposes of principle 5 and principles 8 to 11, information held by an agency includes information that is held outside New Zealand by that agency, where that information has been transferred out of New Zealand by that agency or any other agency.

1298 Resolution on Development of International Standards (29th International Conference of Data Protection and Privacy Commissioners, Montreal, 25–28 September 2007).

1299 Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection (31st International Conference of Data Protection and Privacy Commissioners, Madrid, 4–6 November 2009).

(2) For the purposes of principles 6 and 7, information held by an agency includes information held outside New Zealand by that agency.

(3) Nothing in this section shall apply to render an agency in breach of any of the information privacy principles in respect of any action that the agency is required to take by or under the law of any place outside New Zealand.

In addition, agencies must comply with the use and disclosure principles when sending information to anyone, including overseas.

14.29 Furthermore, where an agency holds information solely as an agent, for the sole purpose of safe custody or for the sole purpose of processing the information on behalf of another agency and does not use or disclose the information for its own purposes, the information is deemed to be held by the agency on whose behalf the information is held or processed.[1300]

14.30 We note that many New Zealanders share personal information directly with overseas companies over the internet. The law of the country where the company is based will govern the way the personal information in question is treated. Many of the reforms discussed in this chapter, with the possible exception of cross-border enforcement cooperation, will therefore have no application to this type of situation.

EU adequacy

14.31 The EU is currently considering the adequacy of New Zealand's privacy laws. New Zealand has not to date been assessed as adequate, there being two main issues that have prevented it. They are:[1301]

- The lack of a prohibition on data export, meaning that New Zealand could be a conduit for personal information through which personal information of EU citizens could be sent on from New Zealand to countries without adequate privacy protections.
- Persons outside New Zealand cannot access their own personal information unless they are citizens or permanent residents.

There have also been several smaller points of concern, including the lack of a "sensitive data" concept in the Act and the inability of individuals to opt out of having their personal information used for direct marketing purposes.[1302] However it appears that these are no longer of such concern.

14.32 There have been efforts to secure legislative amendments to address these issues for many years.[1303] The current Privacy (Cross-border Information) Amendment Bill aims to remove the remaining obstacles to New Zealand achieving adequacy.

1300 Privacy Act 1993, s 3(4).

1301 See, eg, Blair Stewart "International Transfers of Personal Data: Candidate for Adequacy – The New Zealand Case" (Notes for an address to the Privacy Laws & Business 14th Annual Conference, Cambridge, 3 July 2001).

1302 The issue of direct marketing is discussed further in chapter 15.

1303 See, for example, Office of the Privacy Commissioner *Proposed Amendments to the Privacy Act – addressing question of adequacy under EU Data Protection Directive* (15 December 2000) available at www.privacy.org.nz (accessed 8 October 2009).

Privacy (Cross-border Information) Amendment Bill

14.33 The Privacy (Cross-border Information) Amendment Bill is currently before the House. The Bill amends the Act to ensure that New Zealand is not used as a conduit through which personal information can be sent to states without adequate privacy protection. In doing so, the Bill aims to remove the obstacles to achieving EU adequacy noted above. The key changes it introduces are:

- To allow the Commissioner to prohibit a transfer of personal information from New Zealand to another State if she is satisfied, on reasonable grounds, that:
  - the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to the Act; and
  - the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines.[1304]

  This will be achieved by means of a transfer prohibition notice issued by the Commissioner to the agency proposing to transfer the personal information.[1305] Failure to comply with a notice without reasonable excuse will be an offence.[1306]
- To allow the Commissioner to consult with an overseas privacy enforcement authority on complaints that are more properly within their jurisdiction, and to refer the complaint, in whole or in part, to that authority.[1307]
- To remove the current requirement that a person who makes an information privacy request must be a New Zealand citizen or permanent resident, or be in New Zealand.[1308]

14.34 It seems likely that this Bill will pass. This is expected to enable New Zealand to obtain a formal finding of adequacy from the EU.[1309] However, EU adequacy is only one aspect of the issue of trans-border data flows and the Bill's focus is on protections for overseas citizens rather than New Zealanders. The rest of this chapter will consider whether further changes may be needed to deal with trans-border data flows.

EVALUATION OF CURRENT LAW

14.35 As we have seen above, the Act provides some protection where personal information is held overseas. Principle 5 (storage and security) and principles 8 to 11 (accuracy, not keeping personal information longer than necessary, use and disclosure) apply to information held outside New Zealand by an agency. Individuals may, under principles 6 and 7, access and correct personal information held outside New Zealand by an agency.

14.36 If an agency *itself* holds personal information outside New Zealand, principles 5 to 11 apply. If a New Zealand agency sends personal information to overseas agencies that hold information solely as agents, for the sole purpose of safe custody or for the sole purpose of processing information on the New Zealand

1304 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 8 (new s 114B).

1305 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 8 (new s 114C).

1306 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 8 (new s 114E).

1307 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 7.

1308 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 5.

1309 Privacy Commissioner "Report by the Privacy Commissioner to the Minister of Justice on the Privacy (Cross-border Information) Amendment Bill" www.privacy.org.nz (accessed 30 September 2009) para 1.4.

agency's behalf, the information is treated as if it was held by the New Zealand agency itself, so the same rules apply. This would seem to cover the case of outsourcing[1310] and information sent through overseas computer servers.

14.37 If the New Zealand agency gives personal information to an overseas agency, other than one acting as its agent or solely holding or processing information on its behalf, the disclosure to the overseas agency must fall within one of the exceptions to principle 11. If the New Zealand agency does not comply with principle 11, affected individuals could complain to the Privacy Commissioner. However, once the overseas agency has received the information, its holding of it is subject to the laws of the relevant country, which may or may not provide for protection of privacy of the standard expected by New Zealanders.

14.38 It seems to us that this is a potential gap in the law. In transferring personal information to an overseas body, agencies are not required to consider whether the personal information will be adequately protected in the overseas destination. This could expose New Zealanders' personal information to an unacceptable level of risk.

Q162 Should there be more protections around personal information being sent out of New Zealand?

HOW SHOULD THE ACT TREAT TRANS-BORDER DATA FLOWS?

14.39 There are a number of possible general approaches to the question of how trans-border data flows could be regulated, if at all. We begin by considering the broad approach to dealing with trans-border data flows.

Models for dealing with trans-border data flows

14.40 Internationally, a number of approaches exist. These can be roughly grouped into the following categories:[1311]

- no special controls;
- data export controls;
- special exceptions; and
- an accountability model.

No special controls

14.41 As the title suggests, under this approach there are no particular special controls on trans-border data flows. This is the approach taken in the USA.[1312] At present New Zealand and Hong Kong might also be said to fit into this group, although section 10 of New Zealand's Privacy Act could also be considered

1310 Gehan Gunasekara "The 'final' privacy frontier? Regulating trans-border data flows" (2006) 15 IJLIT 362.

1311 These names and groupings were suggested to us by Blair Stewart, Assistant Privacy Commissioner. Another categorisation of models for responding to the challenges of trans-border data flows can be found in Gehan Gunasekara "The 'final' privacy frontier? Regulating trans-border data flows" (2006) 15 IJLIT 362, 378–392.

1312 Although individual organisations may choose to be part of the Safe Harbour Agreement with the EU, whose principles restrict onward transfers of personal information.

to take New Zealand some way towards the accountability model, discussed below. Hong Kong has a section in its law imposing controls similar to the EU, but it has not come into force.

Data export controls

14.42 Under this model, data must not be exported unless it is exported to a country with similar data protection standards to those in the sending country. This is the approach taken in Europe, which we have described above. Argentina[1313] and Australia[1314] (in relation to the private sector) have modelled their laws on the EU in this respect.

14.43 In the most restrictive form of this model, data exports could be prohibited entirely. This is the approach taken in relation to the public sector in British Columbia. Public sector agencies must ensure that personal information they hold is stored in Canada and accessed only in Canada, unless the individual consents or it falls within one of the disclosure exceptions.[1315] Agency heads must report requests for disclosure that come from overseas to the responsible Minister.[1316] This was driven by concerns that information about Canadians could be accessed by US agencies under the USA PATRIOT Act.[1317]

Special exceptions

14.44 This is the approach taken in the Privacy (Cross-border Information) Amendment Bill. It is based upon clause 17 of the OECD Guidelines, which provides:

> A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

Under this model, trans-border data flows are not subject to particular general controls but special exceptions or restrictions can be imposed when the risks warrant it in a particular situation. The Amendment Bill uses the transfer prohibition notice mechanism. Other possible mechanisms could include imposing restrictions on transfers of certain categories of personal information which are particularly sensitive and would not be adequately protected in third countries.

1313 Personal Data Protection Act 2000 No 25.326, art 12.1.

1314 Privacy Act 1988 (Cth), sch 3, cl 9 (National Privacy Principle 9).

1315 Freedom of Information and Protection of Privacy Act RSBC 1996 c 165, s 30.1.

1316 Freedom of Information and Protection of Privacy Act RSBC 1996 c 165, s 30.2.

1317 See Information & Privacy Commissioner for British Columbia *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (Victoria (BC), 2004).

Accountability model

14.45 The accountability model is one that has gained in popularity in recent years. It has been adopted in the APEC accountability principle, discussed above, so can be expected to be influential in the Asia-Pacific region. Under this model, the onus is on an agency to make appropriate arrangements for the protection of personal information if it sends the information overseas. The agency itself will be in breach of the law if it sends information overseas without making such arrangements. New Zealand's section 10 could be seen as following this approach to some extent. It is also the approach taken in Canada, and is likely to be adopted to some extent in Australia and South Africa.[1318]

Canada

14.46 The Personal Information Protection and Electronic Documents Act provides:[1319]

> An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

The Privacy Commissioner can receive complaints about transfers of personal information overseas, and can also audit agencies' practices in this area as part of the Commissioner's general audit function.

14.47 The Privacy Commissioner of Canada has issued guidelines to explain how agencies can fulfil their responsibilities in relation to transfers of personal information to third parties overseas. Agencies must be satisfied that the third party has policies and processes in place, such as staff training and effective security measures, to ensure that the information is protected. The sending agency should also be able to audit or inspect the third party to see how it handles personal information.[1320]

Australia

14.48 The ALRC has proposed a new privacy principle on cross-border data flows that would incorporate the idea of accountability and apply to both public and private sectors. In fact the proposed exceptions mean that the principle is a hybrid of the accountability and data export controls model. The proposed principle states:[1321]

> If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:

1318 South African Law Reform Commission *Project 124: Privacy and Data Protection: Report* (Pretoria, 2009) paras 4.2.26–4.2.37. Also worth noting is the Galway Project, which is devoted to exploring the concept of accountability and how it can fit into broader privacy governance both domestically and internationally: Centre for Information Policy Leadership *Data Protection Accountability: The Essential Elements* (2009).

1319 Personal Information Protection and Electronic Documents Act 2000 c 5, sch 1, cl 4.1.23.

1320 Office of the Privacy Commissioner of Canada *Processing Personal Data Across Borders: Guidelines* (Ottawa, 2009).

1321 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendations 31-1 and 31-2.

(a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to these principles;

(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

(c) agency or organisation is required or authorised by or under law to transfer the personal information.

14.49 The Australian Government has accepted this recommendation, but proposes to modify the exception in (a), adding a requirement that there are accessible mechanisms for individuals to be able to take effective action to have the privacy protections enforced. It also proposes to add the following new exceptions:[1322]

(d) the agency or organisation reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to:

(i) the individual's life, health or safety; or

(ii) public health or public safety

where in the circumstances it is unreasonable or impracticable to seek the individual's consent;

(e) the agency or organisation has reason to suspect that unlawful activity or serious misconduct has been, is being or may be engaged in, and the disclosure of the personal information is a necessary part of its own investigation of the matter or in reporting its concerns to relevant persons or authorities;

(f) the agency or organisation reasonably believes that the disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law.

14.50 Commentators have criticised the proposed exceptions to the accountability principle, suggesting that they are so wide as to make cross-border data transfers effectively unprotected because most will fall within one of the exceptions.[1323] For example, many transfers will take place under a contract, so the principle will not apply (although it might be argued that such contracts will contain adequate safeguards).

Evaluation of models

14.51 All the above models have advantages and disadvantages. The "no special protections" model has the advantages of being simple, requiring no special action and having few compliance costs. However, it is the least effective model in addressing the risks associated with trans-border data flows, leaving New Zealand consumers potentially vulnerable. It also does not meet the expectations of key trading partners, particularly the EU.

1322 Australian Government *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (Canberra, 2009) 77–78.

1323 See, for example, Chris Connolly "Weak protection for offshore data – the ALRC recommendations for Cross Border Transfers" (2008) www.galexia.com (accessed 10 February 2009); Karen Dearne "Privacy changes put data at mercy of scams" (20 October 2009) *Australian IT* www.theaustralian.com.au (accessed 24 February 2010).

14.52 The "data export controls" model is quite common internationally, so there may be benefits in aligning New Zealand with the model seen as international best practice. It is probably the most privacy-protective model, so would offer relatively strong protection for New Zealand consumers. It has the disadvantages of being relatively costly and complex to operate, and may create barriers to trade and cause political tensions with countries such as the USA. It also emphasises borders as an information control point, which can be artificial.

14.53 The "special exceptions" model may take different forms, as outlined above, so potential advantages and disadvantages may vary depending on the form it takes. The model has the benefits of being fairly low cost and likely to be less burdensome for business than other models. It could be seen as targeting the key risk areas. It is also the model already used in the Amendment Bill. Possible disadvantages of this model are that it is uncommon, so may not be trusted by trading partners. It may be seen as providing more limited protection for consumers than more comprehensive data export restrictions. Its exceptional nature means that it may not influence agencies' practices if it was limited to case-by-case exceptions rather than applying to particular classes of information, for example. The one-off exceptions variant of the model is also dependent upon the regulator learning of risks and taking action, so may not prevent all potential problems. Reforms such as audits that we have suggested elsewhere in this paper may help to uncover problems.

14.54 The "accountability" model is consistent with the APEC approach and that of trading partners including Canada and Australia. It has been accepted by the EU in its adequacy finding for Canada. It is a flexible model and gives agencies freedom to find solutions that work for them rather than having external solutions imposed. It also offers a fairly high level of consumer protection. However, it could be viewed as more uncertain than other models.

Options for reform

14.55 Based on the above models, we see a number of potential options for reform. They are:

- remain with the status quo (including the Amendment Bill);
- extend the special exceptions concept so that, for example, transfer prohibition notices could be issued where personal information originates in New Zealand, and/or exports of certain types of information could be restricted;
- impose data export controls, as in the EU; or
- adopt the accountability model.

We are interested in hearing submitters' views on the best approach.

Q163 If you think there should be further reform, which of the approaches discussed in paragraphs 14.40–14.55 do you prefer? Would you prefer another model or variant not discussed here?

CROSS-BORDER ENFORCEMENT COOPERATION

14.56 As noted above, one of the difficulties associated with trans-border data flows is that, when information is sent overseas, Privacy Commissioners will not have the same ability to investigate complaints outside their borders, and individuals may not be able to enforce their rights (such as by making a complaint). People may not know how to complain or who to complain to. Cross-border cooperation between enforcement authorities such as Privacy Commissioners can help mitigate these difficulties, for example by:[1324]

- providing information about foreign laws and ways to get redress;
- coordinating access by consumers to the correct privacy complaints body, for example through a shared web portal;
- sharing information about complaints between enforcement bodies in different countries; or
- empowering domestic complaints bodies to transfer complaints overseas.

14.57 We noted earlier in this chapter that many New Zealanders share personal information directly with overseas companies. Cross-border enforcement cooperation may be able to assist in these situations.

OECD Recommendation

14.58 As we have already noted, the OECD has passed a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. Its broad recommendations include enabling privacy enforcement authorities to better cooperate with overseas bodies; providing mutual assistance through such methods as notification, complaint referral, investigative assistance and information sharing; developing international mechanisms to facilitate cross-border cooperation; and engaging stakeholders in working towards this goal.

14.59 An Annex to the Recommendation provides more detailed guidance, especially on domestic measures that should be taken to enable cross-border co-operation. These include:

- reviewing and adjusting, where needed, domestic laws to ensure their effectiveness for cross-border cooperation;
- considering ways to improve remedies for those harmed by privacy breaches, wherever they occur;
- considering how domestic privacy enforcement authorities might use evidence, judgments and enforceable orders obtained by an overseas privacy enforcement authority to improve their ability to address the same or related conduct; and
- taking steps to ensure that privacy enforcement authorities have authority to deter, investigate and sanction violations of privacy laws.

1324 Blair Stewart "Cross-Border Cooperation on Enforcement Matters" [2004] PLPR 2.

14.60 Of particular note is clause 12, which provides:

> Member countries should take steps to improve the ability of their Privacy Enforcement Authorities to co-operate, upon request and subject to appropriate safeguards, with foreign Privacy Enforcement Authorities, including by:
>
> (a) Providing their Privacy Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to possible violations of Laws Protecting Privacy;
>
> (b) Enabling their Privacy Enforcement Authorities to provide assistance to foreign authorities relating to possible violations of their Laws Protecting Privacy, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved or things.

14.61 The Annex also addresses provision for requesting and giving mutual assistance and collective initiatives to support mutual assistance. This involves naming national contact points, sharing information on enforcement outcomes and participating in enforcement networks. Finally, privacy enforcement authorities are to be encouraged to consult with law enforcement authorities, privacy officers within agencies, civil society and business.

14.62 The New Zealand Act already covers many of these matters. Of particular note is the Commissioner's function of consulting and cooperating with other persons and bodies concerned with the privacy of the individual.[1325] This seems to provide scope for the Commissioner to cooperate with overseas bodies as well as with domestic bodies, although the exact ambit of the power is not clear. In fact the Commissioner's Office is active in international networks of Privacy Commissioners. Furthermore, new section 72C proposed by the Privacy (Cross-border Information) Amendment Bill will allow the Commissioner to refer complaints to overseas privacy enforcement authorities.

14.63 However, some aspects of the Recommendation may not be adequately covered by existing law (together with the Amendment Bill). It is worth considering whether further amendments are desirable. Particular aspects of the Recommendation that may require further implementation are:

- Enabling OPC to share relevant information with overseas privacy enforcement authorities relating to possible violations of privacy law. This is covered to some extent by the existing law and Amendment Bill. However, the Commissioner does not have clear authority to disclose information to overseas bodies and the Amendment Bill focuses on transferring complaints, which is only one aspect of the proposed information sharing.
- Enabling OPC to provide assistance to overseas authorities relating to possible violations of the overseas country's laws. Some limited cooperation could presumably be provided under the general cooperation function, but again clear authority could be beneficial.
- Provision for requesting and giving mutual assistance.
- Cooperation with other authorities and stakeholders. The Act already provides for the Commissioner to refer complaints to the Ombudsmen, the Health and Disability Commissioner and the Inspector-General of Intelligence and

1325 Privacy Act 1993, s 13(1)(j).

Security.[1326] Furthermore, if during or after any investigation the Commissioner believes that there is evidence of a significant breach of duty or misconduct by any agency or officer, employee or member of an agency, the Commissioner is to refer the matter to the appropriate authority. Again, the question is whether this is sufficient. In future, there may need to be power for the Commissioner to share information with bodies such as APEC accountability agents.

- The Human Rights Review Tribunal may also need powers to consider cases with a cross-border element. If such a case came before the Tribunal, there might be evidential issues not currently provided for. Part 4 of the Evidence Act 2006 establishes a procedure where evidence can be taken in Australia for New Zealand court proceedings and vice versa. The Minister has the power to declare a tribunal a court so that it can also use this procedure. Therefore it would seem that this could be used for trans-Tasman cases. The Evidence Act also makes provision for taking evidence in New Zealand for use in civil proceedings overseas, and vice versa. It may be worth considering whether a similar procedure should be available for the Tribunal.

Q164 Does the Act require further amendments to implement the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy? Are any other amendments required in relation to cross-border enforcement cooperation?

IMPLEMENTATION OF APEC PRIVACY FRAMEWORK

14.64 As described above, the APEC Privacy Framework contains ten privacy principles. Implementation is intended to be flexible, so that member economies are not obliged to take a particular approach. The privacy principles in New Zealand's Privacy Act are similar to the APEC Principles, so New Zealand already complies with much of the APEC Privacy Framework. The possible exception to this is the accountability principle, which we have discussed in paragraph 14.22.

14.65 New Zealand's Individual Action Plan notes provisions of the Act that go some way to fulfil the accountability principle, including sections 10 and 3(4) and principle 11. It then goes on to state that:[1327]

> There is no cross-border privacy protection in respect of international transfers of personal information. The Act does not have anything explicit about cross border enforcement cooperation arrangements. Notwithstanding this, the Privacy Commissioner has entered into a Memorandum of Understanding with the Australian Privacy Commissioner which aims to enhance the exchange of information and cooperation between the participants and promote cross border cooperation in investigation and enforcement.

14.66 As discussed above, one option for reform would be to adopt the accountability approach in New Zealand. This would comply with the Framework.

1326 Privacy Act 1993, ss 72–72B.

1327 Asia-Pacific Economic Cooperation *Information Privacy Individual Action Plan: New Zealand (2008)* www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/dp_iaps.Par.0010.File.tmp/Web_IAP_New_Zealand.doc (accessed 2 November 2009).

Cross-border privacy rules

14.67 As discussed above, the Framework envisages the development of a system of cross-border privacy rules (CBPRs), whereby organisations operating across borders would develop their own internal privacy rules to "facilitate responsible and accountable cross-border data transfers" within the organisation. Organisations would still need to comply with local privacy laws.

14.68 It is envisaged that the development of cross-border privacy rules will occur in four steps:

- self-certification by companies that their privacy and security practices comply with the APEC Privacy Framework;
- compliance review of the companies by "accountability agents" that may be APEC-recognised trust marks or government agencies;
- public notification of compliant companies; and
- domestic and cross-border complaint handling and enforcement and cross-border privacy laws.

14.69 A CBPR system is not yet operational in New Zealand.[1328] Having such a system could have a number of benefits for New Zealand agencies and consumers. The potential benefits include that it could:

- provide a clearer framework for businesses to operate across borders;
- be a useful tool to streamline privacy compliance and manage privacy risks for businesses operating across borders
- be used by businesses participating in the system to gain a marketing advantage;
- encourage trade, as businesses may be able to trade more confidently with overseas businesses, and overseas businesses may be able to trade more confidently with New Zealand;
- allow individuals to make an informed choice about the businesses they deal with;
- assist consumers to enforce privacy rights across borders; and
- relieve OPC of some work, as businesses/accountability agents took on more responsibility.

14.70 However, some potential problems could be:

- it could introduce additional complexity that may increase compliance costs and effort for businesses and be confusing for consumers;
- the degree to which businesses want such a system, and would be likely to engage with it, is not clear; and
- there may not be enough privacy experts in New Zealand to perform the various roles required to establish a CBPR system.

1328 We are aware, however, of multinational companies with operations in New Zealand that are developing Binding Corporate Rules, the EU equivalent of CBPRs. It is possible that companies that have BCRs could also have these approved as CBPRs under the APEC Framework.

14.71 Enabling a CBPR system to operate in New Zealand would require consideration of a number of issues, including:

- Who would be the privacy enforcement authority?
- Who would be the CBPR accountability agent(s)?
- What government body would accredit the accountability agent(s)?
- How would businesses engage with the accountability agent(s)?
- What form would certification take?

14.72 The privacy enforcement authority must be a state body. The obvious candidate is the Privacy Commissioner, although alternatives such as the Commerce Commission could be considered.

14.73 The accrediting body for accountability agents must also be a state body. Again, the Privacy Commissioner seems to be a good candidate. Other possibilities might include the Office of the Auditor-General, Audit New Zealand, Standards New Zealand, the Ministry of Economic Development, or a central APEC body.

14.74 Accountability agents could be from the public or private sector. The Privacy Commissioner could also perform this role. There could be a role for the private sector, for example, accountancy firms, law firms or existing overseas trust mark bodies such as TRUSTe. Alternatively, a new entity could be set up to be the accountability agent. This could be, for example, a Crown Company or a trans-Tasman body to audit both Australian and New Zealand businesses.

14.75 The CBPR system may not necessarily require legislation for its establishment. However, some legislative amendments may be required, for example, to ensure that statutory bodies such as the Privacy Commissioner have sufficient authority to perform their roles in the system, or to establish accountability agents. Additional funding may also be required for the agencies chosen to perform the various roles. The system may be able to be partially funded by participating organisations.

Q165 Do you see value in implementing a cross-border privacy rules system in New Zealand? If so, do you have a view on the questions in paragraph 14.71?

Q166 Do you have any further comments on the issues raised by trans-border data flows?

Chapter 15
Direct marketing

15.1 This chapter is concerned with the regulation of direct marketing from the perspective of protecting privacy, and with whether current controls on direct marketing are adequate or whether additional controls are needed. It also looks at the issue of targeted internet advertising based on people's online behaviour.

BACKGROUND

15.2 Direct marketing is the making of marketing approaches to individuals by commercial marketers or businesses, whether New Zealand or overseas based,[1329] by various methods including mail, telephone calls, email (or spam), door-to-door approaches in person, automated dialling machines and, more recently, automated SMS messages. Direct marketing also includes requests for donations to charities, political parties and other groups. Approaches may be made using information obtained from marketing lists, public information (such as phone books or public registers) or information compiled based on previous transactions with the individual.

15.3 The Privacy Act defines direct marketing as:[1330]

> (a) the offering of goods or services; or
>
> (b) the advertising of the availability of goods or services; or
>
> (c) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political, or other purposes,—
>
> by means of—
>
> (d) information or goods sent to any person by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or
>
> (e) telephone calls made to specific persons by name.

1329 The cost of offshore marketing to New Zealand consumers is falling due to internet communications technologies such as Skype. Voice calls are not electronic messages (spam) under the Unsolicited Electronic Messages Act 2007, sch, clause 1.

1330 Privacy Act 1993, s 9(2). The definition has no current purpose in the Act and it was used to exempt the application of principle 11 to disclosures before 1 July 1996 of personal information collected before 1 July 1993 for direct marketing purposes. However, the definition is used in the Telecommunications Information Privacy Code (discussed below). See *Necessary and Desirable* para 2.17.

15.4 The Code of Practice for Direct Marketing in New Zealand defines "direct marketing" as the process by which consumers are offered the opportunity to obtain or purchase goods or services or make charitable donations direct by mail, newspaper, magazine, radio, television, telephone, facsimile, email, Internet or any similar means of communication.[1331]

15.5 Direct marketing may be either solicited or unsolicited. Solicited marketing is marketing to an individual that has been authorised, often in advance, as part of an existing relationship with a business or organisation (that is, the marketing of further products or services) or in response to enquiries.

15.6 Direct marketing is a useful tool for businesses in distributing information about their products and services and gaining new customers. It therefore has an important role in contributing to the economic performance of businesses and the economy as a whole. Marketing initiatives can benefit consumers by informing them of new products and pricing, including discounts, and this information flow can therefore improve economic efficiencies between buyers and sellers of products and services, as well as competition between businesses, to the benefit of the market.

15.7 While some individuals actively welcome marketing approaches, some forms of marketing are more intrusive than others and may have negative effects on the individuals to whom they are targeted. The question is whether the current rules achieve the right balance between business, economic and individual interests and whether the current regulatory tools need to be adjusted or supplemented to achieve a reasonable balance.

How direct marketing affects privacy

15.8 Unwanted direct marketing is often experienced as a nuisance. One initial question is whether it is a privacy intrusion. In an earlier report, we concluded that it was probably more accurate to describe receiving unwanted marketing material as an irritant than an invasion of privacy, at least in the context of using information from public registers for marketing purposes.[1332] Some see it as an intrusion – in other words, an invasion of spatial privacy. Apart from this, however, New Zealanders have expressed concern about how their personal information is treated by businesses. In a 2008 survey commissioned by the Privacy Commissioner, 90 per cent of New Zealanders surveyed were concerned (including 74 per cent very concerned) if a business they did not know got hold of their personal information. The survey also found that 88 per cent were concerned (including 72 per cent very concerned) if a business asked them for personal information that does not seem relevant to the purpose of the

1331 Marketing Association "Code of Practice for Direct Marketing in New Zealand" reviewed October 2009 www.marketing.org.nz (accessed 15 December 2009).

1332 New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008) para 4.65.

transaction, while 86 per cent were concerned (including 73 per cent very concerned) if a business they supplied their personal information to for a specific purpose used it for another purpose.[1333]

15.9 According to Daniel Solove's "Taxonomy of Privacy", things like spam, junk faxes and telemarketing are examples of intrusions into people's private affairs.[1334] The South African Law Commission, in considering the nature of direct marketing, found it to be an accepted fact that there is a privacy dimension in the collecting and using of information for purposes not agreed to by the data subject and certain harmful aspects of personal information handling (such as misleading conduct in the collection and use of personal information).[1335]

15.10 The Australian Law Reform Commission (ALRC) conducted a phone-in in 2006 and found that 3 out of 4 callers nominated unsolicited telemarketing as their number one privacy complaint: "People face a barrage of information, emails and messages all day. They want their home to be a sanctuary and see telemarketing calls as an unwanted intrusion into their private life."[1336] The ALRC has also noted that the issue of direct marketing and its regulation provokes strong responses:[1337]

> On the one hand, there is a strong push from consumers and consumer advocates to tighten the rules on direct marketing to make it more difficult for companies engaged in direct marketing to communicate with people in this way, particularly with respect to unsolicited direct marketing. This draws on the conceptualisation of privacy as including, at least, "the right to be let alone." On the other hand, business groups and others have emphasised the importance of direct marketing for the economy generally. They have also stressed that, if direct marketing is carried out appropriately, it can be of considerable assistance to consumers that receive direct marketing communications. It is possible to balance these competing positions by recognising that some forms of direct marketing can be pernicious and can erode individuals' privacy rights but that, if undertaken appropriately, direct marketing also can be beneficial.

15.11 Another dimension is the growing trend towards the use of targeted or behavioural internet advertising as a form of marketing to internet users. Behavioural internet advertising is discussed further below. On the one hand, behavioural advertising seeks to reduce the annoyance factor to consumers by sending relevant advertising messages to the consumer. However, targeting is achieved through compiling profiles of information about consumers' online activities and preferences. In the 2008 survey commissioned by the Privacy Commissioner, two thirds of New Zealanders surveyed were uncomfortable or very uncomfortable about internet search engines and social networking sites tracking internet use and emails in order to deliver targeted advertising.[1338]

1333 Office of the Privacy Commissioner *Individual Privacy and Personal Information Survey 2008* www.privacy.org.nz (accessed 13 January 2010).

1334 Daniel J Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477, 522.

1335 South African Law Reform Commission *Project 124: Privacy and Data Protection: Report* (Pretoria, 2009) 343.

1336 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 891.

1337 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 26.27–26.29.

1338 Office of the Privacy Commissioner *Individual Privacy and Personal Information Survey 2008* www.privacy.org.nz (accessed 13 January 2010).

THE REGULATION OF DIRECT MARKETING UNDER THE PRIVACY ACT

15.12 Direct marketing can be regarded as impacting on informational privacy where it involves the use of someone's personal details for an unwanted purpose. The next question to consider is therefore the extent to which direct marketing is regulated by the Privacy Act. The Privacy Act does not provide any specific controls on direct marketing, but applies the generic concepts that the use of personal information should be authorised by the person concerned and there should be transparency around the use of people's personal information. Whether direct marketing is regulated by the Privacy Act depends partly on whether marketing approaches are based on the use of "personal information" as defined in the Privacy Act. For example a telephone number, physical address, or an email address is not necessarily "personal information" unless it is linked to other information such as a person's name through which an individual becomes identifiable.

15.13 Even where information used for marketing approaches is "personal information", it may be able to be freely used or disclosed for marketing purposes by virtue of exceptions to the privacy principles such as consent (including a generic consent at the time that personal information is collected from an individual),[1339] or where the personal information is publicly available, for example from the phone book or a public register,[1340] or where use or disclosure of the personal information for marketing purposes is a purpose for which it was collected (or a directly related purpose).

15.14 Nevertheless, privacy principle 10 as it applies to telecommunication agencies[1341] has been adapted by rule 10 of the Telecommunications Information Privacy Code 2003 to provide specific controls on direct marketing in that:[1342]

- A telecommunications agency may use telecommunications information for another purpose if authorised by the individual concerned, but if the other purpose is for direct marketing, this is only permitted if the individual has been advised that he or she may withdraw such authorisation at any time.[1343]
- A telecommunications agency must not, without consent, use traffic data (such as dialling information) obtained as a result of interconnection, wholesaling or similar arrangements between network operators for the purposes of direct marketing to an individual who is not a subscriber of the agency.[1344] This was directed towards a practice where a customer of one company placing a call to a customer of another company would receive marketing from that company inviting them to switch networks.

1339 See New Zealand Marketing Association *Guide to the Privacy Act 1993* www.marketing.org.nz/cms/Resources/105 (accessed 3 December 2009): "Direct marketers can buy, rent or exchange personal information, but it must be with the authority of the individual."

1340 See New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008) paras 4.54–4.59.

1341 These include including network operators, telecommunication service providers, directory publishers, directory enquiry agencies, internet service providers, call centres and mobile phone retailers: Telecommunications Information Privacy Code 2003, rule 4(2).

1342 See Office of the Privacy Commissioner *Privacy on the Line – Privacy in Telecommunications* (Wellington, 2000) 11–13.

1343 Telecommunications Information Privacy Code 2003, rule 10(1)(b).

1344 Telecommunications Information Privacy Code 2003, rule 10(2).

15.15 Where the use of personal information for marketing purposes is in breach of the privacy principles, one issue is the suitability and efficiency of the Privacy Act enforcement framework to respond to an issue involving mass use of personal information. The Privacy Act enforcement framework is based on individual complaints that require investigation to determine whether the marketing complained of was authorised by the individual or subject to any other exception to the principles. Authorisation may be difficult to trace due to changes of business policies, the repackaging of information into marketing lists and the sharing of marketing lists between companies. Investigations are therefore not straightforward and may not prove to be cost-effective in relation to the level of individual harm suffered. It is difficult for the Privacy Commissioner to deal with marketing complaints holistically where the issue raised may involve a mix of Privacy Act and non-Privacy Act issues (depending on whether the information used is personal information or not). The Privacy Commissioner's limited resources also mean that marketing complaints cannot always receive priority.

15.16 One question for consideration therefore is whether direct marketing requires a parallel enforcement measure that is more comprehensive, practical, cost-effective and consumer-friendly. If, as proposed in chapter 8, the Privacy Commissioner is given the power to issue enforcement notices, that will constitute one method of enforcement. In this chapter we outline other possible enforcement measures that have been introduced in other countries, such as express controls on direct marketing in data protection legislation that give consumers an express right to opt out of receiving direct marketing on a case-by-case basis, and, in relation to telemarketing, Do Not Call registers established by statute establishing a comprehensive opt-out right. These measures shift the focus from the resource-intensive investigation of privacy complaints to providing a practical consumer-controlled remedy. Investigation of breaches can then centre on whether there has been compliance with expressed opt-out preferences.

OTHER CONTROLS ON DIRECT MARKETING

15.17 The Unsolicited Electronic Messages Act 2007 controls the sending of unsolicited email, text messages and instant messaging, requiring an opt-in by the recipient before a organisation can send commercial electronic messages, and providing an opt-out for other promotional messages. The Act does not cover spam sent by fax, or voicemails. Internet service providers are required to deal with complaints about spam, with the Department of Internal Affairs having powers to investigate and enforce the Act.

15.18 The Harassment Act 1997 provides that one type of harassment is making contact with a person (whether by telephone, correspondence, or in any other way).[1345] A further act of harassment is giving offensive material to a person, or leaving it where it will be found, given to, or brought to the attention of, that person.[1346] To qualify as harassment, there must be at least two separate specified acts within a 12 month period.[1347]

15.19 The Telecommunications Act 2001 contains an offence for the use of a telephone to disturb, annoy or irritate someone, whether by calling up without speech or by wantonly or maliciously transmitting communications or sounds, with the

1345 Harassment Act 1997, s 4(1)(d).

1346 Harassment Act 1997, s 4(1)(e).

1347 Harassment Act 1997, ss 3 and 4.

intention of offending the recipient.[1348] However it is unlikely that direct marketing calls would trigger this offence, even in the case of repeated contact after the individual has expressed a request not to be further contacted. Only in unusual circumstances would direct marketing calls be "wanton" or "malicious", or be made with the intention to offend.

15.20 The Marketing Association of New Zealand (in conjunction with the Advertising Standards Authority) has issued a Code of Practice for Direct Marketing in New Zealand, in consultation with the Ministry of Consumer Affairs, the Ministry of Economic Development, the Commerce Commission and the Consumers' Institute.[1349] Principle 4 of the Code provides that marketers are to carry out their business in a way that is socially responsible. The Marketing Association maintains Do Not Mail (DNM) and Do Not Call (DNC) registers containing details of consumers who have requested no unasked for mail and/or telephone calls. The Code requires member marketers to check the list of people they plan to communicate with against the DNM and DNC registers and remove names from the prospecting lists if they appear on these registers, unless the person is an existing customer or has opted to receive marketing communications.[1350] In addition, calls may not be made to unlisted or unpublished numbers without the consumer's permission.[1351] The Code requires member marketers to provide individuals with an opportunity to opt out of receiving marketing information they have not requested and to have systems in place to effect opt-outs.[1352] Two shortcomings of the voluntary scheme noted by the Privacy Commissioner are that it is confined only to members of the association and that it lacks enforcement mechanisms.[1353]

15.21 The Marketing Association has also issued a Code of Practice for Telemarketing that requires telemarketers to remove a person's name from the telephoning list and lists offered to other organisations if requested to do so, and to inform the person about the DNC register.[1354] Otherwise there is no obligation on marketers to inform individuals about the DNC scheme. This Code also provides that automatic dialling systems are not to be used to call residential lines.[1355]

1348 Telecommunications Act 2001, s 112.

1349 Marketing Association "Code of Practice for Direct Marketing in New Zealand" www.marketing.org.nz (accessed 15 December 2009).

1350 Marketing Association "Code of Practice for Direct Marketing in New Zealand" www.marketing.org.nz (accessed 15 December 2009), principle 4(b).1.

1351 Marketing Association "Code of Practice for Direct Marketing in New Zealand" www.marketing.org.nz (accessed 15 December 2009), principle 5(c).3.

1352 Marketing Association "Code of Practice for Direct Marketing in New Zealand" www.marketing.org.nz (accessed 15 December 2009), principle 4(b).3.

1353 *Necessary and Desirable* para 2.9.13.

1354 Marketing Association "Telemarketing Code of Practice" www.marketing.org.nz (accessed 15 December 2009).

1355 Marketing Association "Telemarketing Code of Practice" www.marketing.org.nz (accessed 15 December 2009), principle 4(m)(a).

15.22 Other guidance issued by the Marketing Association includes:

- Best Practice Guidelines for Fax Marketing;[1356]
- 6 Guiding Principles for Responsible Email Marketers;[1357]
- Best Practice Guidelines for Mobile Marketing;[1358]
- Standards for Search Engine Marketing;[1359]
- Best Practice Guidelines Direct Marketing Data;[1360] and
- Privacy Guidelines for Data Co-operatives.[1361]

15.23 An initiative of the Data Advisory Network (a special interest group of the Marketing Association) is the List Warranty Register which provides assurance to the marketing community that marketing lists provided by organisations participating in the scheme[1362] are compliant with the Privacy Act and the Marketing Association's best practice guidelines.[1363]

MARKET RESEARCH

15.24 Market research is "the systematic gathering and interpretation of information about individuals or organisations using the statistical and analytical methods and techniques of the applied social sciences to gain insight or support decision making."[1364] Market research is an activity that shares some features of direct marketing. Like direct marketing, unsolicited contact from market researchers can be considered as a nuisance or irritant. However, some people are willing to provide personal information more freely for research purposes than for direct marketers.

15.25 The Privacy Act applies to the collection of personal information for the purposes of market research. In addition, the Market Research New Zealand Code of Practice applies to members of Market Research New Zealand and contains privacy provisions relating to privacy policies, collection of data, use of data, security of processing, rights of the respondent, and trans-border transactions. In particular, researchers are not to disclose personal identities of respondents to their clients or to disclose personal information to their clients unless the respondent has expressly consented and provided that this will not result in direct marketing and other commercial activities. More generally, researchers

1356 Marketing Association "Best Practice Guidelines for Fax Marketing" www.marketing.org.nz (accessed 15 December 2009).

1357 Marketing Association "6 Guiding Principles for Responsible Email Marketers" www.marketing.org.nz (accessed 15 December 2009).

1358 Marketing Association "Best Practice Guidelines for Mobile Marketing" www.marketing.org.nz (accessed 15 December 2009).

1359 Marketing Association "Standards for Search Engine Marketing" www.marketing.org.nz (accessed 15 December 2009).

1360 Marketing Association "Best Practice Guidelines Direct Marketing Data" www.marketing.org.nz (accessed 15 December 2009).

1361 Marketing Association "New Zealand Privacy Guidelines for Data Co-operatives" (adapted from the ADMA Privacy Principles for Data Co-operatives) www.marketing.org.nz (accessed 15 December 2009). The guidelines provide that "sensitive information" cannot be used by a data co-operative without proof of express consent, and that shared data may only be transferred to other countries where the data will be used consistently with the Privacy Act 1993.

1362 Inaugural List Warranty Register participants are Acxiom, DataMarket, New Zealand Post, Veda Advantage and PMP Micromarketing.

1363 Marketing Association "List Warranty Register" www.marketing.org.nz (accessed 15 December 2009).

1364 Code of Practice of the Market Research Society of New Zealand Inc, revised June 2008.

are never to allow personal data collected in a market research project to be used for any purpose other than market research. However, some market research may be carried out by non-members who are not bound by the code.

OVERSEAS REGULATORY CONTROLS

Privacy principles and data protection legislation dealing with direct marketing

15.26 The EU Data Protection Directive requires direct marketers to inform people that their data may be collected and used for direct marketing, and to give them the right to opt out.[1365] The Data Protection Act (UK) contains an express right to prevent processing for purposes of direct marketing:[1366]

> An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

15.27 The United Kingdom has also enacted a specific direct marketing regime within the Privacy and Electronic Communications (EC Directive) Regulations 2003. These regulations supplement the Data Protection Act[1367] and provide for direct marketing controls on:

- the use of automated calling systems to make calls to individual or corporate subscribers without prior consent;[1368]
- the use of fax machines to send direct marketing messages to individual or corporate subscribers;[1369]
- unsolicited calls to individual or corporate subscribers if a subscriber has opted out;[1370] and
- unsolicited email to individual subscribers without prior consent.[1371]

15.28 The regulations also require the Office of Communications (Ofcom)[1372] to maintain a do-not-fax (FPS) register[1373] and a do-not-call (Telephone Preference Service or TPS) register of phone numbers (including mobile numbers) where

1365 European Parliament and Council Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data [1995] OJ L281.

1366 Data Protection Act 1998 (UK), s 11.

1367 If personal data is processed for marketing (e.g. if the name of the person receiving the message is known), compliance with the Data Protection Act is required. In addition, any direct marketing has to comply with the regulations (not just direct marketing involving the processing of personal information).

1368 Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), reg 19.

1369 Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), reg 20 requires opt-in for individual subscribers and allows opt-out for corporate subscribers.

1370 Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), reg 21.

1371 Although there is a "soft opt-in" exception that allows direct marketing where contact details are obtained in the course of a sale or negotiations for sale of a product or service, the direct marketing relates only to similar products and services and a simple means of opt-out is given on each occasion: Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), reg 22.

1372 Ofcom is the UK telecommunications and broadcasting regulator.

1373 Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), reg 25.

subscribers (individual or corporate) do not wish to receive unsolicited calls.[1374] There is no exemption from the TPS for not-for-profits. Enforcement of the regulations is through extension of Part V of the Data Protection Act.[1375]

15.29 In Germany, a recent amendment to the Federal Data Protection Act requires marketers to get consumers' consent to use their address data unless:

- the brand has an existing relationship with the consumer; or
- the source of the third party data is clearly stated on the direct mail envelope.

There are also exemptions for business-to-business marketing, charity direct marketing, political direct marketing and using data from public directories to market a company's own products.[1376]

15.30 In Australia, the National Privacy Principles (NPPs) (which apply to the private sector) deal with the issue of direct marketing by organisations as part of the use and disclosure principle.[1377] NPP 2.1(c) permits the use of personal information for the secondary purpose of direct marketing only if:

- the information in question is not "sensitive information";
- it is impracticable to seek the individual's consent;
- the organisation will not charge the individual for giving effect to a request by the individual not to receive direct marketing communications;
- the individual has not requested the organisation to refrain from providing direct marketing communications;
- in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that the individual may express a wish not to receive any further direct marketing communications; and
- each written direct marketing communication to the individual sets out the organisation's business address and telephone number and, if the communication is made by electronic means, a number or address at which the organisation can be contacted electronically.

15.31 In addition to direct marketing permitted by NPP 2.1(c), there are other circumstances in which the use or disclosure of personal information for direct marketing is permitted under the NPPs. These are where:

- the individual consents to the direct marketing;
- the information was collected for the primary purpose of direct marketing; or
- the direct marketing is related (or directly related in the case of sensitive information) to the primary purpose of collection, and the individual concerned would reasonably expect the organisation to use or disclose the information for direct marketing.

1374 Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), reg 26.

1375 As well as dealing with various forms of direct marketing, the regulations also deal with a range other matters.

1376 Noelle McElhatton "German direct marketers grapple with new opt-in law" (5 August 2009) *Marketing Direct* www.brandrepublic.com (accessed 25 February 2010).

1377 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 26.9.

15.32 The ALRC has recommended that direct marketing be dealt with in the Australian Privacy Act under a specific privacy principle:[1378]

> **UPP6.1 Direct marketing (only applicable to organisations)**[1379]
>
> 6.1 An organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:
>
> (a) individual would reasonably expect the organisation to disclose the information for the purpose of direct marketing; and
>
> (b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications.
>
> 6.2 An organisation may use of disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:
>
> (a) either the:
>
> (i) individual has consented; or
>
> (ii) information is not sensitive and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;
>
> (b) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications; and
>
> (c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and
>
> (d) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual or the source from which it acquired the individual's personal information.
>
> 6.3 In the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:
>
> (a) comply with the requirement within a reasonable period of time; and
>
> (b) not charge the individual for giving effect to the request.

The Australian Government has accepted this recommendation with some minor amendments.[1380]

15.33 In Queensland, the Information Privacy Act 2009 requires decision makers to take steps to protect personal information before disclosing it if they reasonably believe the recipient of the information will use it to market directly to an individual.[1381]

1378 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 26.1.

1379 An "organisation" includes an individual, body corporate, partnership, unincorporated entity and a trust.

1380 Australian Government *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (Canberra, 2009) 56.

1381 Information Privacy Act 2009 (Qld), sch 3, cl 11(4).

Do Not Call registers

15.34 In the United States, the Federal Trade Commission (FTC) established a do-not-call register in 2003 and has over 191 million registrations.[1382] The US register does not apply to charities, market research companies or political polling. Marketing is also permitted if there is an existing business relationship, for a limited 18 month period, unless the consumer opts out.

15.35 A Do Not Call List has also been established in Canada.[1383] There are exemptions for charities, political parties, newspaper subscriptions and surveys. There have been some problems with the Do Not Call list such as misuse, lack of oversight, and inadequate policing mechanisms.[1384] It has since been reported that the Do Not Call List is to be replaced by giving consumers the chance to opt in, rather than opting out of telemarketing schemes, under the proposed anti-spam Electronic Commerce Protection Act.[1385]

15.36 In Australia, the Do Not Call Register Act 2006 took effect in May 2007.[1386] Individuals can list their Australian fixed line or mobile phone numbers on the DNC Register, provided that those numbers are used mainly for private or domestic purposes. Registration allows individuals to opt out of receiving a wide range of direct marketing calls.[1387] Registrations are valid for 3 years and can be withdrawn at any time. In addition, the Australian Communications and Media Authority (ACMA) has issued a national industry standard for telemarketing and research calls which restricts the times of day at which calls may be made.[1388] The full direct costs of operating and maintaining the DNC register are recovered from industry through fees for accessing the register that are set using cost-recovery principles.[1389]

15.37 From 31 May 2007, it became illegal, in the absence of consent, for any non-exempt telemarketer in Australia and overseas to contact a number listed on the register. ACMA is responsible for overseeing the register's operation and investigating breaches.[1390] Enforcement options include issuing a formal warning,

---

1382 Federal Trade Commission *Biennial Report to Congress Pursuant to the Do Not Call Registry Fee Extension Act of 2007* (December 2009) 3.

1383 An Act to Amend the Telecommunications Act 2005 c 40 came into force on 30 June 2006.

1384 See Chris Connolly and Amy Vierboom *Emerging Best Practice in Do Not Call Registers* (Galexia, Sydney, 2009) 5–6. A privacy commentator, Michael Geist set up the iOptOut website to highlight the shortcomings of the Do Not Call List: Michael Geist "Do-not-call faces challenges" (7 April 2008) *thestar.com* www.thestar.com (accessed 9 April 2008).

1385 Michael Geist "The Untold Story of Do-Not-Call Enforcement (aka Why Killing Do-Not-Call Can't Come Fast Enough)" (27 April 2009) www.michaelgeist.ca (accessed 19 May 2009).

1386 500,000 Australians signed up in the first 3 days of the register's operation.

1387 A survey found that 79 per cent of people surveyed reported fewer telemarketing calls since registering their home number on the Do Not Call Register: Australian Communications and Media Authority "Community Attitudes to Unsolicited Communications" (Newspoll Research Report, Sydney, 2009) 30.

1388 Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007 (Cth).

1389 Australian Communications and Media Authority "ACMA invites comment on new industry fees and payment methods to access the Do Not Call Register in 2009–10" (24 March 2009) Media Release 35/2009.

1390 ACMA has reported a 60 per cent drop in complaints about calls to numbers on the Do Not Call Register, indicating a significant improvement in compliance by telemarketers: Australian Communications and Media Authority "Complaints about unwanted telemarketing calls plummet" (6 July 2009) Media Release 81/2009.

accepting enforceable undertakings, issuing an infringement notice, which specifies a financial penalty, or commencing proceedings in the Federal Court or Federal Magistrates Court.[1391] The Australian Do Not Call scheme is currently under review.[1392]

15.38 While national legislation cannot necessarily protect against direct marketing calls from other countries, it does offer some recourse against the use of offshore call centres by local companies. In Australia, an Australian company was penalised under the Do Not Call Register legislation after an offshore call centre made calls on its behalf to numbers on the Do Not Call Register.[1393] The Federal Trade Commission also states that it can take action against US companies that solicit sales through overseas telemarketers.[1394]

15.39 In New Zealand, there is a voluntary scheme, in the form of the Marketing Association Do Not Call scheme which members of the Association are obliged to check against any prospective marketing list for new customers. The scheme relies on members' internal complaint handling procedures. Because of the limitations of the voluntary scheme, there have been calls for a comprehensive legislative scheme. The Privacy Commissioner has recommended that consideration be given to the merits of a national system, established under statute, to control the use of automated dialling machines and enable individuals to opt out of telemarketing.[1395]

15.40 The Marketing Association has argued that a government-run register is unnecessary. Its Do Not Call scheme has about 44,000 numbers on it and about 500 are added each month.[1396] While the Privacy Commissioner has been supportive of industry initiatives directed towards better practices, the association's register only applies to its own members and so does not control telemarketing by non-members. Massey Marketing professor Janet Hoek has called for do-not-call legislation, arguing that the New Zealand Marketing Association register is not widely publicised and many consumers would not know of its existence:[1397]

> Government regulation is more visible and the options it creates are better known. In addition, government regulation is pro-active rather than reactive; unlike self-regulation it provides explicit compliance incentives in the form of penalties, and, most importantly, it is completely independent, which promotes consumer confidence in the outcomes.

1391 Australian Communications and Media Authority "Dodo pays penalty for calling numbers on the Do Not Call Register – Backgrounder" (22 October 2008) Media Release.

1392 Australian Government Department of Broadband, Communications and the Digital Economy *Discussion Paper: Do Not Call Register Statutory Review* (Canberra, 2009).

1393 See also "Frequently Asked Questions About the Do Not Call Register: Are telemarketing calls from overseas covered by the register?" www.donotcall.gov.au (accessed 19 May 2009).

1394 Federal Trade Commission "Q&A: The National Do Not Call Registry: Q32: Are telemarketing calls from overseas covered?" www.donotcall.gov (accessed 13 January 2010).

1395 *4th supplement to Necessary and Desirable* recommendation 25B; Claire Trevett "Database Suggested to Limit Cold Calls" (5 July 2008) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 25 February 2010).

1396 See Chris Connolly and Amy Vierboom *Emerging Best Practice in Do Not Call Registers* (Galexia, Sydney, 2009) 10, noting that countries such as New Zealand that rely on self-regulatory options have very low numbers of registered numbers, compared to government run registers.

1397 Massey University "Call for Laws Banning Tele-marketers" (8 May 2007) Press Release.

15.41 The United Future Party has announced a party policy to create a national Do Not Call register to apply to all profit-making companies, and to ban telemarketers from calling anyone after 9pm or on Sundays.[1398]

REFORM OPTIONS

15.42 The current regulatory regime for direct marketing in New Zealand consists of a number of elements:

- a comprehensive regime for direct marketing by email under the Unsolicited Electronic Messages Act that requires consumer opt-in to authorise unsolicited commercial messages, including an enforcement regime administered by the Department of Internal Affairs;
- coverage under the Privacy Act to the extent that information used for marketing approaches is personal information, with a complaints procedure administered by the Privacy Commissioner; and
- voluntary Marketing Association Code of Practice including Do Not Call and Do Not Mail schemes that provide an opt-out option for consumers.

With regard to the Marketing Association Code, enforcement relies on members' own internal complaint-handling procedures, and the Code does not apply to non-member marketers.

15.43 The issue we have identified is whether the gaps in the current regulatory regime are such that a reform option should be considered. In our view, an efficient user-friendly remedy for people affected by direct marketing approaches of various kinds should be available. While such a remedy is available in the case of electronic commercial spam and under the Marketing Association DNC and DNM schemes, these cover specific types of direct marketing (email) or specific participants (members of the Marketing Association) rather than providing a comprehensive remedy. The Privacy Commissioner's complaints process does not currently lend itself to marketing complaints and is only available where marketing is based on the use of personal information. Various exceptions to the privacy principles also reduce the scope for complaints about direct marketing to be made under the Privacy Act. We raise a number of possible reform options for consideration. In addition to these, our proposal in chapter 8 that the Commissioner be able to issue enforcement notices is likely to be a useful remedy in relation to direct marketing.

15.44 As we have noted, there is currently a separate regime for unsolicited email. It may be worth considering as part of any reform whether the treatment of spam should be aligned with the treatment of direct marketing using other media.

Privacy Act: introducing a right to opt out of direct marketing

15.45 The are a number of ways in which the Privacy Act could be amended to provide individuals with a mechanism to be able to opt out from direct marketing. This could be by:

- introducing a new direct marketing privacy principle (as per the ALRC's recommendation);
- providing for the right to opt out in a section of the Privacy Act (as per the UK Data Protection Act);

1398 United Future NZ Party "'Do Not Call' register United Future policy" (14 July 2008) Press Release.

- providing an additional limit on disclosure for the purpose of direct marketing (as per the Queensland Information Privacy Act);
- supplementing principle 7 (the correction principle) with a right to block the use of personal information for direct marketing purposes (as recommended by the Privacy Commissioner);[1399]
- issuing a Code of Practice that could adapt the privacy principles and their exceptions as they apply to direct marketing (such as notice and consent), address the use of sensitive personal information for marketing purposes, and provide for individuals to have the ability to opt out; or
- amending Schedule 2 to the Telecommunications Information Privacy Code 2003 to allow subscribers to opt out of marketing based on use of subscriber directories.[1400]

Any of these options would require agencies to maintain their own do not contact lists to keep track of consumers who have opted out and would allow consumers to opt out of direct marketing on a case-by-case basis.

Do Not Call register

15.46 This option would involve a centralised Do Not Call register, allowing consumers to effect a comprehensive opt-out from telemarketing, rather than company-by-company. Consumers could then opt in to direct marketing by particular companies on a selective basis. Options to consider are:

- continuing with the voluntary approach under the Marketing Association Do Not Call scheme (status quo);
- retaining voluntary membership of the Marketing Association, while requiring all marketers by statute to comply with the Do Not Call scheme; and
- setting up a statutory Do Not Call scheme with enforcement processes.

15.47 If a statutory scheme is proposed, consideration would need to be given to the following matters:

- the statutory vehicle that would establish the register (the Privacy Act or separate legislation or regulation);
- the responsible agency to administer the register (the Privacy Commissioner, a consumer protection agency or another agency), bearing in mind that the regulator and the operator of the register need not necessarily be the same agency; and
- whether the statutory scheme would be established on a self-funding basis or whether, and if so how, the scheme would require respective contributions by industry and government.

Scope of regulatory measures

15.48 In relation to the possible options outlined above, consideration would need to be given to whether there should be different requirements depending on whether the marketing is commercial or non-commercial (such as charitable,

1399 *Necessary and Desirable* recommendation 25.

1400 See for example the proposal of the South African Law Reform Commission *Project 124: Privacy and Data Protection: Report* (Pretoria, 2009) 365–366.

not-for profit, political or market research). For example, the Unsolicited Electronic Messages Act covers all forms of spam, but imposes additional requirements in relation to commercial spam.[1401]

Q167 Are any regulatory controls on direct marketing needed? If so, which forms of direct marketing require further controls:

- telemarketing;
- unsolicited mail;
- door-to-door marketing;
- autodialing;
- electronic spam;
- fax marketing;
- charitable solicitations;
- political donation solicitations; or
- other?

Q168 Which regulatory option or options do you favour:

- a direct marketing principle in the Privacy Act;
- a right to opt out of direct marketing in the Privacy Act, a Privacy Act code of practice, or regulations;
- a voluntary or compulsory Do Not Call Register for telemarketing; or
- any other option?

BEHAVIOURAL INTERNET ADVERTISING

15.49 Behavioural internet advertising is targeted internet advertising, based on information collected from people's use of the internet.[1402] Information collected can include Web sites and pages within those sites visited by an individual, the time and duration of the visits, search terms entered into search engines, internet purchases, and responses to advertisements.[1403] It is a process which is typically invisible to consumers.[1404] The information is collected from online searches and web browser profiles created by search engines such as Google and network advertisers through the use of cookies and Web bugs.[1405]

15.50 The stated benefits of behavioural advertising include free online content supported by advertising, personalisation of ads, and the potential reduction in unwanted advertising, while stated privacy risks include invisibility of data collection and the shortcomings of current disclosure practices, the potential to develop and store detailed profiles, and the risk that data is used for unanticipated

1401 Unsolicited Electronic Messages Act 2007, ss 10 and 11.

1402 See New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 128–130.

1403 Federal Trade Commission *Online Profiling: a Report to Congress* (Washington, DC, 2000) 4.

1404 Federal Trade Commission Staff Report *Self-Regulatory Principles for Online Behavioural Advertising* (Washington, DC, 2009) ii.

1405 In relation to online profiling, see Federal Trade Commission *Online Profiling: a Report to Congress* (Washington, DC, 2000); Electronic Privacy Information Center "Privacy and Consumer Profiling" www.epic.org (accessed 22 June 2009).

purposes or falls into the wrong hands.[1406] Some people view targeted advertising as more useful and less annoying than random ads, especially if they are offered discounts. But others are uneasy about the collection of details of their internet usage, finding it intrusive: "An extensive data collection and targeting infrastructure has emerged, one that poses significant threats to the privacy – and personal autonomy – of hundreds of millions".[1407] One commentator has suggested that: "The question boils down to this: How much information – and what type of information – should companies be able to collect and utilise about people while they are online?"[1408] Another industry commentator notes: "We have to work out in society what we believe is a good exchange."[1409] Several mergers between US internet companies and advertising companies have intensified concerns about the exploitation of consumer data for advertising purposes.

15.51 Specific types of behavioural advertising include (i) "first party" or "intra-site" behavioural advertising where a website collects consumer information to deliver targeted advertising at its site, but does not share any information with third parties; and (ii) contextual advertising which targets advertisements based on the Web page a consumer is viewing or a search query the consumer has made, but involves little or no data storage. The more privacy-intrusive form of behavioural advertising, however, is the tracking of consumers by network advertisers via cookies on multiple websites which then serve advertisements based on the consumer's web-based interactions:[1410]

> Every web page's individual views, every word typed in a search query box (also known as the "database of consumer intentions"), every video download, and every word in an email may create one more data point that a marketer can leverage and use to more precisely target the audience with customized media placement and messaging.

15.52 Behavioural advertising by internet service providers uses deep-packet inspection rather than the cookie-based model. Deep-packet inspection is even more wide reaching as it can allow the targeting of ads based on substantially all the websites a consumer visits rather than a more limited number of websites visited within a network of particular websites.[1411]

1406 Federal Trade Commission Staff Report *Self-Regulatory Principles for Online Behavioural Advertising* (Washington, DC, 2009) i–ii.

1407 Center for Digital Democracy and the US Public Interest Research Group "Complaint and Request for Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices" (Washington, DC, 2006) 48. A Californian study found that 85 per cent of respondents thought that sites should not be allowed to track their behaviour around the Web to show them ads: see Louise Story "To Aim Ads, Web is Keeping Closer Eye on You" (10 March 2008) *New York Times* www.nytimes.com (accessed 11 March 2008).

1408 Renee Boucher Ferguson "A Battle is Brewing Over Online Behavioural Advertising" (27 March 2008) www.eweek.com (accessed 13 January 2010).

1409 Zachary Britton, quoted in Associated Press "Doubts arise over ISP ad targeting" (2 September 2008) *The Sydney Morning Herald* www.smh.com.au (accessed 3 September 2008).

1410 Center for Digital Democracy and the US Public Interest Research Group "Supplemental Statement in Support of Complaint and Request for Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices" (Washington, DC, 2007) 5.

1411 Deep packet inspection is discussed in chapter 13.

Behavioural advertising and personal information

15.53 Behavioural advertising does not fit neatly into the data protection framework because the information collected for profiling purposes may not be "personal information" as defined in the Privacy Act. The information collected often does not include the consumer's name, physical address or similar identifier that could be used to identify the consumer in the offline world. Instead, businesses generally use cookies to track consumers' activities and associate those activities with a particular computer or device.

15.54 Privacy advocates have suggested that personal information in this context should be any information that can, directly or indirectly:[1412]

- identify an individual, including but not limited to name, address, IP address, assigned identifier, or a combination of unique or non-unique identifying elements associated with a particular individual that can be reasonably associated with a particular individual; or
- permit a set of behaviours or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier.

Similarly, the Federal Trade Commission has commented that in the context of online behavioural advertising, the traditional notion of what constitutes personal information is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data.[1413]

15.55 In the United Kingdom, the view of the Information Commissioner is that profiles based on information collected by cookies which is then linked to other information which uniquely identifies the individual is personal information and is covered by the Data Protection Act.[1414]

15.56 In chapter 3 we discuss whether Internet Protocol addresses can be considered to be personal information, and note that this depends on a case-by-case assessment.

1412 Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearinghouse and World Privacy Forum Submission to Federal Trade Commission in advance of Town Hall, "Behavioural Advertising: Tracking, Targeting and Technology" (Washington, DC, 1–2 November 2007) www.worldprivacyforum.org (accessed 16 December 2009).

1413 Federal Trade Commission Staff Report *Self-regulatory principles for online behavioural advertising* (Washington, DC, 2009) 21.

1414 Information Commissioner's Office (UK) *Data Protection Good Practice Note: Collecting personal information using websites* (London, 2007).

Regulatory and other responses to behavioural advertising

15.57 Arguments have been made against additional regulation for online behavioural advertising:[1415]

> Good public policy requires that the benefits of more information be balanced against the benefits of greater privacy. Regulation should be undertaken only if a market is not functioning properly and if the benefits of new measures outweigh their costs. Our analysis suggests that proposals to restrict the amount of information available would not yield net benefits for consumers.

15.58 Nevertheless, in various countries, there have been a range of regulatory responses and proposals in relation to the issue of behavioural advertising.

European Union

15.59 The EU has called for advertisers to come up with a voluntary code of conduct to protect consumer and privacy rights but has signalled that EU authorities will probably have to legislate to prevent abuses. New EU legislation will require users to consent to cookies being stored on their computers.[1416]

United Kingdom

15.60 The Internet Advertising Bureau (IAB) has developed Good Practice Guidelines for Online Behavioural Advertising, based on the three core principles of notice, user choice and education.[1417] Each IAB member is to:

- provide clear and unambiguous notice that it collects data for the purposes of online behavioural advertising;
- provide an approved means for consumers to decline online behavioural advertising from that member;
- provide a clear and unavoidable statement to the user about the product and offer the user a choice about whether or not to be involved, where specific consent to the collection and use of data for online behavioural advertising is required by law;
- make information available and easily accessible to educate users about online behavioural advertising; and
- refrain from creating online behavioural advertising segments intended for the sole purpose of targeting children under the age of 13.

The principles are stated to complement and in some cases supplement the UK legal framework provided by the Data Protection Act and the Privacy and Electronic Communications Regulations. The Privacy and Electronic

1415 Thomas M Lenard and Paul H Rubin *In Defense of Data: Information and the Costs of Privacy* (Technology Policy Institute, Washington, DC, 2009).

1416 "Europe Approves New Cookie Law" (11 November 2009) http://blogs.wsj.com (accessed 13 November 2009).

1417 Internet Advertising Bureau *Good Practice Guidelines for Online Behavioural Advertising* www.iabuk.net (accessed 7 December 2009).

Communications (EC Directive) Regulations 2003, prohibit the use of cookies and tracking systems to collect any information without notice and the opportunity to opt out (subject to exceptions).[1418]

15.61 The All-Party Parliamentary Communications Group has conducted an inquiry considering such questions as whether the Government should be intervening over behavioural advertising services, either to encourage or discourage their deployment, or whether this is a matter for individual users, internet service providers and websites. As a result of the inquiry, the Group (comprising MPs and Lords from all parties) called for a change in the law to make it illegal to engage in behavioural advertising without an internet user's explicit, informed consent. The Group considered the IAB Good Practice Guidelines to be inadequate as they are based on the idea of opt-out rather than explicit opt-in. Behavioural targeting of children and young people was a particular concern.[1419]

15.62 The Office of Fair Trading has launched a market study into online targeting of advertising and pricing which will cover behavioural advertising and customised pricing.[1420] This may ultimately lead to an industry code of practice.

United States

15.63 The Federal Trade Commission (FTC) has been examining behavioural advertising and the privacy issues raised over a number of years, conducting a series of public workshops,[1421] issuing reports, and bringing enforcement actions challenging deceptive privacy claims and improper disclosure of consumer data.[1422]

15.64 In February 2009 the FTC released "Self-Regulatory Principles for Online Behavioural Advertising" following extensive consultation with stakeholders. The principles promote prominent disclosure separate to privacy policies, ideally combined with education programmes. The governing concepts of the principles are:

- transparency and control: companies collecting information for behavioural advertising should provide meaningful disclosures to consumers about the practice and choice about whether to participate;
- reasonable security and limited data retention;
- material changes to privacy policies: before a company uses behavioural data in a way that is materially different from promises made when the data was collected, it should obtain express consent from the consumer; and

1418 Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), reg 6.

1419 All Party Parliamentary Communications Group *Can we keep our hands off the net? Report of an Inquiry by the All Party Parliamentary Communications Group* (London, 2009).

1420 Office of Fair Trading (UK) "OFT launches market studies into advertising and pricing practices" (15 October 2009) Press Release 126/09. It is expected that the study will be completed by the UK summer 2010.

1421 A Privacy Roundtable on privacy issues posed by technology and business practices that collect and use consumer data, including behavioural advertising, was held on 9 December 2009. See Federal Trade Commission www.ftc.gov (accessed 17 December 2009).

1422 For example, an enforcement action was brought against Sears for failing to adequately disclose the scope of personal information collected via a downloadable software application that not only tracked online browsing but also monitored online secure sessions and some computer activities not related to the internet. See Federal Trade Commission "Sears Settles FTC Charges Regarding Tracking Software" (6 April 2009) www.ftc.gov (accessed 22 June 2009).

- consent prior to use of sensitive data (opt-in), such as information about children, health and finances.

15.65 The principles are not limited to personal information but include any data collected for online behavioural advertising that could reasonably be associated with a particular consumer or with a particular computer or device. The FTC has recently made addressing behavioural targeting a high priority and has signalled that there may be changes, which may or may not involve regulation.[1423]

15.66 Congress has also held hearings into online advertising and deep packet inspection.[1424] While the collection of online information from children is restricted under the Children's Online Privacy Protection Act, various Bills to regulate online behavioural advertising to the general population have been and continue to be drafted. Recent legislative proposals would require that websites that collect information about visitors, or use an outside company to do so, in order to target advertising would be required to prominently disclose what information they gather and how it is used. [1425] Visitors would be required to be able to opt out of having their data collected. Furthermore, websites that share user information with outside advertising networks would be required to obtain user approval before collecting data, except in certain cases. Websites that collect sensitive personal information would also be required to obtain consent first.

15.67 Privacy groups have proposed a Do Not Track List, administered by the FTC. One survey found 72 per cent of American internet users would opt out of online tracking if they could.[1426] The Future of Privacy Forum has announced a major research initiative to examine different methods for communicating with users about online advertising and privacy practices, and will explore potential tools and notices that companies could use to raise consumer awareness about the use of online behavioural advertising data.[1427]

15.68 The Code of Practice for Direct Marketing in New Zealand provides that:

- when consumers are required to provide personal information on a website, they must be given the opportunity to choose not to have such information made available to others for marketing purposes;[1428] and

1423 See, for example, Stephanie Clifford "Fresh Views at Agency Overseeing Online Ads" (5 August 2009) *New York Times* www.nytimes.com (accessed 25 February 2010). See also critique and recommendations of the Center for Democracy and Technology "Online Behavioural Advertising: Industry's Self-regulatory Framework is Necessary, But Still Insufficient on its Own to Protect Consumers" www.cdt.org (accessed 13 January 2010).

1424 Stephanie Clifford "Congress Looks into how Online Companies Track Consumers" (18 June 2009) http://mediadecoder.blogs.nytimes.com (accessed 25 February 2010).

1425 See, for example, Kate Kaye "Web Privacy Bill could come by November" (1 October 2009) www.clickz.com (accessed 5 October 2009).

1426 Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy *Americans Reject Tailored Advertising and Three Activities That Enable It* (Social Science Research Network Working Paper, 2009) 10.

1427 "Future of Privacy Forum Announces Research Initiative to Develop Effective Messages to Communicate with Users About Online Data Use" (19 May 2009) www.futureofprivacy.org (accessed 17 June 2009).

1428 Marketing Association of New Zealand "Code of Practice for Direct Marketing in New Zealand" principle 5(d).3.

- consumers are to be advised if information that could identify them is collected that will be linked with click-stream data (such as that obtained from their behaviour, pathway or choices expressed when visiting a website) and how it will be used.[1429]

Industry responses

15.69 Some companies, including Google, Yahoo! and Microsoft, have developed tools to allow consumers to opt out of receiving targeted online advertisements.[1430] Other technologies available include opt-out cookies, a technical means of opting out of targeted advertising, and cookie alternatives.[1431] Another proposed measure is to develop a symbol that advertisers would display on advertisements to denote that they collect data from users.[1432]

Reform Options

15.70 The practice of collecting information from internet use to deliver targeted advertising raises the following issues:

- it is not always transparent to internet users that data generated by their internet activity will be collected and used for marketing purposes;
- Privacy Act coverage can be uncertain due to the limits of the definition of "personal information," as well as cross-border issues;[1433] and
- while the practice is covered by voluntary standards to some extent, application of the standards depends on whether personal information is also collected and not on the collection of click-stream data per se, observance of these standards is limited to Marketing Association members, and the standards rely on internal complaint-handling procedures rather than statutory enforcement processes.

15.71 Possible responses to behavioural advertising might include the following:

- The Privacy Commissioner could continue to provide information to consumers about behavioural advertising to increase awareness of the practice and its privacy implications, and options for consumers to protect their online privacy.
- The Privacy Commissioner could issue information or guidance about how the privacy principles apply to behavioural advertising and encourage privacy-friendly practices including privacy-enhancing technologies.
- The Privacy Commissioner could make statements about behavioural targeting practices that are privacy-intrusive.

1429 Marketing Association of New Zealand "Code of Practice for Direct Marketing in New Zealand" principle 5(d).5.

1430 See Saul Hansell "A Guide to Google's New Privacy Controls" (12 March 2009) http://bits.blogs.nytimes.com (accessed 25 February 2010).

1431 See Stephanie Olsen "New Technology Serves Ads Sans Cookies" (3 April 2009) *CNET News* http://news.cnet.com (accessed 12 June 2009); Daniel C Howe and Helen Nissenbaum "Trackmenot: Resisting Surveillance in Web Search" in Ian Kerr, Carole Lucock and Valerie Steeves (eds) *Lessons from the Identity Trail: Privacy, Anonymity and Identity in a Networked Society* (Oxford University Press, New York, 2009).

1432 See, eg, Saul Hansell "Seeking a Symbol for 'This Ad Knows About You'" (3 December 2009) http://bits.blogs.nytimes.com (accessed 25 February 2010).

1433 Cross-border issues are discussed in chapter 14.

- The Privacy Commissioner could call on the Marketing Association and/or the Advertising Standards Authority to develop voluntary standards drawing on standards developed overseas that meet with her approval.
- The Privacy Commissioner could invite the Marketing Association and/or the Advertising Standards Authority to develop a Code of Practice for behavioural advertising for approval under the Privacy Act.
- Legislative changes to the Privacy Act could be considered.

It may be preferable to see what form of regulation emerges in other jurisdictions before implementing higher level regulatory options such as legislative change.

Q169 Do you have any comments about the privacy issues associated with online behavioural targeting? What, in your view, is the appropriate regulatory response to these issues?

Chapter 16

Data breach notification

16.1 This chapter discusses the practice of data breach[1434] notification and the merits of introducing a mandatory data breach notification requirement into the Privacy Act.

16.2 The chapter begins by explaining the meaning of a data breach and explaining the practice of breach notification. It then outlines the current legal framework and reform proposals in New Zealand and in other common law jurisdictions. The chapter closes by explaining, in more detail, the aspects that make up a data breach notification scheme, and poses a number of policy questions that we seek responses to.

16.3 Currently, the holders of personal information, both public and private sector agencies, are under no legal obligation to notify individuals or the Office of the Privacy Commissioner when individuals' personal information is compromised, notwithstanding that notification is said to provide individuals the opportunity to minimise the negative consequences that can come from a data breach, such as identity theft or fraud or discriminatory treatment. The fact that notification does not always occur is not surprising given the lack of incentives for companies to notify affected individuals including the potential costs to its financial bottom line and reputation.

16.4 The security of an individual's personal information is becoming increasingly important as more and more information of a sensitive or private nature is being collected and retained by both public and private sector agencies. Given the mass of information that is now being collected and held by organisations, it is inevitable that at certain times private information of individuals will be accessed, found, or otherwise inappropriately acquired. The question is what, if anything, agencies should be required to do in such cases.

1434 We use the terms "data breach" throughout this chapter as it is often colloquially associated with the topic in mass media and much of the literature we have reviewed. Other references include "security breach", "information security breach", "data security breach", and "privacy breach" (the last being the term used by the New Zealand Office of the Privacy Commissioner).

WHAT IS DATA BREACH NOTIFICATION?

16.5 Simply put, a data breach is the "unauthorised access to or collection, use or disclosure of, personal information."[1435] Breach notification "is the practice of notifying affected individuals when their personal information has become available to unauthorised individuals or organisations."[1436]

16.6 Data breaches take on a multitude of forms ranging from the innocent loss of a file to a more egregious act aimed at damaging another individual. Some involve individuals' intentional acts to usurp the personal details of others, whereas others may be more innocent and involve nothing more than an employee mistakenly accessing personal information on a company's shared computer work space. Data breaches can involve loss or theft of personal information or equipment on which personal information is stored (including CDs, USB keys, and other portable storage devices), inappropriate access controls allowing unauthorised use, equipment failure, human error, unforeseen circumstances such as a fire or flood, a hacking attack, or through "blagging" offences where personal information is obtained by deceiving the organisation which holds it.[1437]

16.7 Data breach notification laws are a ubiquitous feature of the US privacy law landscape. They were pioneered in California in 2003[1438] and exist in approximately 45 other States and the District of Columbia.[1439] Many US laws only relate to the private sector. Moreover, they exist without the support of broad-based privacy laws such as New Zealand's Privacy Act. Voluntary notification guidelines exist in many countries, which apply in some cases to both public and private sector agencies, and require notification in a range of situations. Voluntary guidelines exist in Australia,[1440] Canada,[1441] New Zealand,[1442] and in the United Kingdom.[1443]

16.8 Amongst the US laws and various guidelines, distinctions exist particularly in regard to:[1444]

- who is covered (for example, whether they apply to both the public and private sectors);

1435 Office of the Privacy Commissioner *Information Paper to accompany Privacy Breach Guidance Material* (Wellington, February 2008) 1.

1436 Office of the Privacy Commissioner *Information Paper to accompany Privacy Breach Guidance Material* (Wellington, February 2008) 1.

1437 Information Commissioner's Office *Guidance on Data Security Breach Management* (London, March 2008) 1.

1438 California Civil Code § 1798.29.

1439 www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws (accessed 9 November 2009).

1440 Office of the Privacy Commissioner (Cth) *Guide to Handling Personal Information Security Breaches* (Sydney, August 2008).

1441 Office of the Privacy Commissioner of Canada *Key Steps in Responding to Privacy Breaches* (Ottawa, 2007).

1442 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008).

1443 Information Commissioner's Office *Guidance on Data Security Breach Management* (London, March 2008).

1444 Fred Cate "Information Security Breaches – Looking Back and Thinking Ahead" (The Centre for Information Policy Leadership, 2008) 4.

- what types of information are covered (for example, whether medical information is included and whether it includes combinations of information);
- the circumstances that must exist to "trigger" notification (for example, acquisition of personal information or acquisition and a serious risk of harm to an individual);
- the timing, content, and method of notification;
- any other parties that need to be notified, such as relevant regulators including Privacy Commissioners;
- whether data encryption will be an exemption to the requirement to notify;
- the penalties for non-compliance; and
- whether or not a civil cause of action is available against agencies that fail to notify.

We discuss some of these aspects of breach notification laws in more detail below.

DATA BREACH CASES

16.9 The number of data breaches that occur in New Zealand each year is difficult to gauge. While breaches are reported from time to time in the media, and the Privacy Commissioner has reported to us that notifications are received in her office, there are no accurate data available. Overseas experience in comparable jurisdictions would suggest that data breaches occur regularly (whether or not all are detected).

16.10 In New Zealand recent high profile data breach examples include the Treasury losing a CD in the post that contained the personal and company tax details of numerous individuals;[1445] the mobile phone network provider 2degrees' website suffering teething problems making it possible to see the personal details of previous visitors to its site;[1446] and Massey University's intranet suffering a fault in its security system thereby potentially exposing the sensitive information of students to anyone who accessed the site.[1447] Instances of police officers inappropriately accessing the national intelligence computer have also been recorded.[1448]

16.11 Numerous large scale data breaches have been recorded overseas, most notably in the United Kingdom and the United States. High profile cases in the United Kingdom include Her Majesty's Revenue and Custom Service losing two CDs containing 25 million records containing financial and other details of people in receipt of child benefits (including names, addresses, dates of birth, and national insurance numbers).[1449] Another case involved the United Kingdom Ministry of Defence losing a laptop computer containing the sensitive personal details of 600,000 recruits or potential recruits.[1450] It was also found that the CD contained the further personal

1445 "Treasury Loses CD with Tax Information" (20 September 2009) www.tvnz.co.nz (accessed 18 February 2010).

1446 "Security Flaw Hits 2degrees Website" (5 August 2009) www.stuff.co.nz (accessed 18 February 2010).

1447 Albany Students' Association "Massey Uni Experiences Serious Breach of Security" (1 April 2009) Press release, available at www.scoop.co.nz (accessed 18 February 2010).

1448 Ian Steward "Police Computer Violations Exposed" (7 December 2009) *The Press* Christchurch www.stuff.co.nz (accessed 18 February 2010).

1449 Richard Thomas and Mark Walport *Data Sharing Review Report* (London, July 2008) 9.

1450 UK Information Commissioner *Enforcement Notice to Secretary of State Defence* (14 July 2008) 1.

information of up to another 400,000 individuals, totalling approximately 1,000,000 people.[1451] Similar large data breach incidents occur in the US. Daily, stories of large data breaches appear on the internet and in other media.[1452]

THE CASE FOR DATA BREACH NOTIFICATION

16.12 In this part of the chapter we lay out some of the justifications given to support the need for breach notification, as well as some of the criticisms that have been made in response.

Common rationales

Identity theft and identity fraud

16.13 Data breaches can involve all types of information, from the benign to the particularly sensitive. Some information is inherently sensitive and its loss can be costly and devastating to the individuals concerned. Other information may be relatively insignificant on its own, but can become more sensitive when viewed in combination with other information. Certain types of information may, if found in the wrong hands, put other people in danger of harm, including physical, financial, and reputational harm.[1453] The loss of medical records containing personal medical history could lead to discriminatory treatment or ostracism. Exposing an individual's physical address may expose them to threats of physical harm or threats to their personal privacy. The loss of bank account details could result in financial harm including fraud and identity theft.

16.14 The link between breaches of personal data and identity fraud and identity theft has been the primary justification submitted in the US in support of notification laws. Given the vast range of highly personal information that is now being collected and held by both public and private sector agencies, the possibility of that data being breached, and subsequently being used in identity fraud is said to be growing.[1454] Identity crime in the New Zealand context is discussed in chapter 17.

16.15 Notification is said to be necessary and justified as it enables the individuals whose information has been compromised to take steps to mitigate and control the negative effects that can result from a breach. This could involve changing bank account numbers and passwords, monitoring credit reports and bank account transactions, or taking steps to retrieve the information that was lost. Notification of a data breach is said to be particularly necessary given that an individual is usually unaware of its occurrence, unlike the case of car theft for example, where the owner is usually immediately aware that their vehicle is missing. Notifying an individual in cases where an agency knows or suspects information has been compromised would partially overcome this problem.

1451 UK Information Commissioner *Enforcement Notice to Secretary of State Defence* (14 July 2008) 2.

1452 See for example two databases containing lists of data breaches and the number of customers affected in each case at www.datalossdb.org (accessed 27 October 2009) and www.privacyrights.org/ar/ChronDataBreaches.htm (accessed 27 October 2009).

1453 Uniform Law Conference of Canada *Report of the Joint Criminal/Civil Section Working Group on Identity Theft: A discussion Paper* (Charlottetown, 2007) 14.

1454 However some challenge this premise. See, for example, Fred Cate "Information Security Breaches – Looking Back and Thinking Ahead" (The Centre for Information Policy Leadership, 2008) 4.

Reducing other harms

16.16 While the risk of identity theft and identity fraud have been the primary justifications for mandatory breach laws in the US, those outside of the US tend to focus on the full range of harms in their justifications. These include stalking, embarrassment, ostracism, or discrimination that could result from the release or loss of information held by an organisation. Notification enables individuals to take steps to mitigate these harms.

The "right to know"

16.17 As well as providing practical benefits to individuals affected by data breaches, a requirement to notify can also be justified as a matter of principle on the basis of a "right to know."[1455] This principle dictates that individuals are owed a moral obligation from any agency that is collecting, storing, or using those individuals information, to be informed if it is compromised in any way. Simply put "individuals whose personal information has been exposed to potential unauthorized use as a result of a security breach deserve to be notified".[1456]

16.18 If an organisation is benefiting from or required to use the personal information of an individual it is right for society to expect that that information is reasonably protected and to expect to be notified when that information is compromised. In relation to private organisations which benefit from the personal data of individuals it is right to expect that they are prepared to let individuals know when their information is compromised. In relation to agencies of the state, the argument is stronger given the particularly sensitive information the state holds about individuals that they are at times required by law to provide. Proper information handling practices in both the public and private sector should be encouraged.

16.19 A further aspect of the "right to know" is the notion that individuals should not be the "last to know" about a data breach involving their personal information, for example by reading of the breach in the newspaper. Prompt notification enables potentially embarrassing or damaging consequences to be mitigated through early response action taken by the individual concerned.

Policy development, research, and sector oversight

16.20 As well as benefiting affected individuals, it has also been said that breach notification can "enable law enforcement, researchers, and policy makers to better understand which firms and sectors are best (or worst) at protecting consumer and employee data."[1457] In this regard notification assists in understanding the privacy and security environment and aids the development of policy in this area.

1455 Sasha Romanosky, Rahul Telang, Alessandro Acquisti "Do Data Breach Disclosure Laws Reduce Identity Theft?" (Carnegie Mellon University, 2008) 2.

1456 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 22.

1457 Sasha Romanosky, Rahul Telang, Alessandro Acquisti "Do Data Breach Disclosure Laws Reduce Identity Theft?" (Carnegie Mellon University, 2008) 2.

This would be so particularly if the Privacy Commissioner had a function of publicly notifying breaches (even in an anonymised form) as it would alert everyone to the size of the problem.

Data breach law criticisms

Ineffectiveness of data breach laws

16.21 While supporters of mandatory data breach notification rely on the preceding justifications to argue that data breach laws are necessary, some criticise the laws as an inappropriate response to the problem of data breaches and identity theft.

16.22 There is little evidence to date that mandatory breach notification laws have led to a reduction of data breach incidents.[1458] This could suggest that mandatory breach notification laws are an ineffective way to encourage agencies to adequately protect information, or may otherwise be due to the relative youth of mandatory breach laws worldwide.

16.23 In the case of identity theft, one of the few studies conducted on the link between data breach notification laws and identity theft concluded that the effect of these laws on the reduction of identity theft was marginal.[1459] The authors compared the extent of identity fraud in US States that have data breach notification laws with those that do not. They concluded that "we find that the adoption of data breach disclosure laws have marginal effect on the incidences of identity thefts and reduce the rate by just under 2 per cent on average."[1460] This is important to note as it brings in to question the justification for breach laws based on the perceived link between data breaches and identity theft and fraud.

Outmoded response

16.24 A possible reason for the marginal effect on identity theft or the lack of effect in reducing breach incidents can be found in the criticisms of data breach laws by Fred H Cate. In his work on data breach laws, he criticises the approach being taken to protect data breaches and identity theft as a "twentieth century approach to twenty first century information flows and challenges."[1461] Largely in response to the US data breach laws, he questions whether or not data breach notifications are really an appropriate response given the ubiquitous use and exchange of digital data that occurs in the world today. He considers that notifications

1458 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 22.

1459 Sasha Romanosky, Rahul Telang, Alessandro Acquisti "Do Data Breach Disclosure Laws Reduce Identity Theft?" (Carnegie Mellon University, 2008) 11.

1460 Sasha Romanosky, Rahul Telang, Alessandro Acquisti "Do Data Breach Disclosure Laws Reduce Identity Theft?" (Carnegie Mellon University, 2008) 16.

1461 Fred Cate "Information Security Breaches – Looking Back and Thinking Ahead" (The Centre for Information Policy Leadership, 2008) 19.

were designed for a time when "data processing was infrequent, highly centralised, and clearly structured."[1462] Now, in relation to this "bottomless ocean of information" he states that:[1463]

> notices are too slow, too cumbersome, and too poorly timed to provide meaningful protection for information security, and requiring them as a broad response to security threats promises to inundate individuals with notices they are ill-equipped and unlikely to act on.

16.25 Cate does note that a number of proposals, including the New Zealand guidelines, "reflect many of the practical lessons from the broad and diverse U.S. experiences about the advantages and limits of notice"[1464] and avoid many of the criticisms he poses (which are directed particularly at the EU and US approaches). However, his general point cannot be entirely dismissed.

Unnecessary burdens

16.26 Some critics of data breach laws have suggested that they are costly and constitute a regulatory burden on organisations with little concomitant benefit to consumers. It is also said that these laws can be costly and time consuming for individuals who receive data breach notifications and may take unnecessary and often inappropriate responses.[1465] Some figures quoted suggest that the probability of a single data breach being misused is very small, bringing into question the need to notify in many cases.[1466]

NEW ZEALAND Legal requirements

16.27 Neither the Privacy Act, the Privacy Principles, nor any of the codes require mandatory breach notification. This means that agencies are not required to notify individuals whose personal information has been compromised, no matter how sensitive the information, and no matter how serious the risk of harm that could be suffered as a result.

16.28 The Privacy Commissioner has made clear however that failure to notify affected individuals could be a factor that is taken into account if a complaint is received concerning a breach of principle 5.[1467] Principle 5 requires holders of personal information protect information by such security safeguards as it is reasonable in the circumstances to take. If an individual was to become aware that their

1462 Fred Cate "Information Security Breaches – Looking Back and Thinking Ahead" (The Centre for Information Policy Leadership, 2008) 19.

1463 Fred Cate "Information Security Breaches – Looking Back and Thinking Ahead" (The Centre for Information Policy Leadership, 2008) 2.

1464 Fred Cate "Information Security Breaches – Looking Back and Thinking Ahead" (The Centre for Information Policy Leadership, 2008) 1.

1465 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 22.

1466 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 22.

1467 *4th Supplement to Necessary and Desirable,* recommendation 23A, para 2.5.

own personal information had been compromised and make a complaint, the Privacy Commissioner may take a failure to notify that individual into account in considering whether the organisation involved took all reasonable steps.[1468]

The guidelines

16.29 In August 2007, the Office of the Privacy Commissioner issued voluntary data breach guidelines – *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* ("the guidelines") – for consultation. The guidelines were finalised and released in February 2008.[1469]

16.30 The guidelines state that a privacy breach is "the result of the unauthorised access to or collection, use or disclosure of, personal information." "Unauthorised access" is access that contravenes the terms of the Privacy Act.[1470] The guidelines are separated into four steps:

- breach containment and preliminary assessment;
- evaluation of the risks associated with the breach;
- notification; and
- prevention.

16.31 As the list above illustrates, these guidelines go further than requiring notification as a response, making them more comprehensive than various US State requirements. The guidelines present a proactive approach and stress that breach prevention and data security is the most effective means of protecting the privacy of individuals. Notification is one aspect of a wider set of recommendations aimed at the protection and security of personal information.

16.32 The guidelines do not require notification in all cases, and outline a series of "threshold" questions that must be considered before recommending that affected individuals be notified. Matters that should be taken into account include the nature of the information that has been breached, particularly the level of sensitivity of that information, its context, whether or not the information is encrypted, anonymised, or otherwise inaccessible, and how the information can be used and whether this includes fraudulent or harmful purposes. As well as this, an organisation should consider who is affected by the breach, and finally, assess whether harm could foreseeably result, either to an individual, the organisation in question, or the public. Importantly, the guidelines note that the "key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to an

1468 See for example Case Note 211257 [2009] NZPrivCmr 16 – concerning complaints lodged with the Privacy Commissioner after a member of a government agency lost a file on the street containing a list that included personal information about a large group of people. In this case, the Privacy Commissioner found that while there was a breach of principle 5, there was no interference with privacy because the individuals involved suffered no harm. In the case the agency took steps to mitigate any harm that could have resulted from the breach, by expediently notifying the affected individuals and the Privacy Commissioner's Office, seeking and receiving legal undertakings from media outlets who obtained the files not to publish their details and getting the original file back with the help of the police.

1469 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008).

1470 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 1.

individual whose personal information has been inappropriately accessed, collected, used or disclosed."[1471] More detailed comments about the guidelines are included later in the chapter where appropriate.

16.33 The guidelines are relatively new and it is not yet possible to tell what effect they are having on data protection practices in either the public or private sector (if any). It may be that mandatory notification laws should only be considered an option after there has been a proper opportunity to assess the effectiveness of the voluntary guidelines.

OTHER JURISDICTIONS

16.34 Mandatory notification laws exist in nearly every US State,[1472] and almost 30 of these are based on the original Californian model.[1473] Various attempts to enact a federal breach notification law have, to date, been unsuccessful. Financial institutions throughout the US are subject to mandatory notification obligations under the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* issued by the Department of the Treasury.[1474]

16.35 The EU has recently amended its e-data Directive covering its telecoms sector (including phone, email, SMS, and internet use) to include a mandatory notification requirement.[1475] Calls to require mandatory notification across all sectors were not followed, but the European Commission has stated publicly that it will consider this in the future.[1476] An all-sector mandatory notification law has also recently been enacted in Germany.[1477]

16.36 No mandatory breach notification laws exist in Australia at either a federal or a state level but the Australian Law Reform Commission (ALRC) recently recommended that "the Privacy Act should be amended to include a new Part on data breach notification."[1478] This recommendation was supported by the Australian Office of the Privacy Commissioner.[1479] The Australian Government is yet to respond to this aspect of ALRC's report.[1480]

1471 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 6.

1472 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.14.

1473 www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws (accessed 9 November 2009).

1474 Department of the Treasury (US) *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

1475 EC Directive 2009/136/EC.

1476 Viviane Reding, Member of the European Commission Responsible for Information Society and Media "Securing Personal Data and Fighting Data Breaches" (Speech to EDPS-ENISA Seminar, Brussels, 23 October 2009).

1477 Bundesdatenschutzgesetz [Federal Data Protection Act], 20 December 1990, BGBl. I at 2954, as amended. The German law requires that affected individuals must be notified of any unlawful or unauthorised access of personal information if the incident threatens significant harm to the individual.

1478 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.73.

1479 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.51.

1480 However it has signalled that it will respond in due course. See Australian Government *First Stage Response to the Australian Law Reform Commission Report 108 – Australian Law Reform Commission For Your Information: Australian Privacy Laws and Practice* (October 2009).

16.37 No mandatory breach notification laws exist in the United Kingdom where mandatory breach laws were rejected by the authors of the *Data Sharing Review Report*[1481] and the UK Government.[1482]

16.38 No mandatory breach law exists in Canada (with the exception of Ontario[1483]), but the House of Commons Standing Committee on Access to Information, Privacy and Ethics has recommended that a mandatory notification regime be added to Canada's Personal Information Protection and Electronic Documents Act 2000 (PIPEDA).[1484] This recommendation was supported by the Canadian Government[1485] and Privacy Commissioner.[1486] Two sets of voluntary breach notification guidelines exist in Canada at the Federal level. One set is issued by the Treasury Board of Canada and applies to the Privacy Act 1985 and the other is issued by the Canadian Privacy Commissioner[1487] and applies to PIPEDA.[1488] The New Zealand guidelines are explicitly based on the guidelines issued by the Privacy Commissioner of Canada.

OPTIONS FOR REFORM

Our view

16.39 The Law Commission currently hold no firm view as to the need for mandatory breach notification but are interested in your views. We have laid out a series of questions below that would be helpful if the decision is taken to recommend that mandatory breach notification requirements should be enacted in New Zealand law.

Mandatory vs voluntary notification

16.40 Earlier in the chapter we outlined some of the commonly stated justifications for notifying individuals. Here we briefly outline the case for and against a *mandatory* notification regime.

16.41 If matters are left to voluntary notification, there are incentives not to notify. Notifying individuals in response to a data breach is likely to involve costs for organisations, both in terms of the actual costs of making the notification and costs to its reputation, as well as potential penalties from regulators and the possibility of costly civil claims bought against the organisation by affected individuals.[1489]

1481 The *Data Sharing Review Report* was commissioned by the UK Government to undertake a review of the framework for the use of personal information in both the public and private sectors. See Richard Thomas and Mark Walport *Data Sharing Review Report* (London, July 2008) recommendation 11.

1482 Ministry of Justice (UK) *Response to the Data Sharing Review Report* (London, November 2008) 11.

1483 In Ontario mandatory notification is required in relation to health records under the Personal Health Information Act 2004 (Ontario), s 12.

1484 House of Commons Standing Committee on Access to Information, Privacy and Ethics (Can) *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics – Statutory Review of the Personal Information Protection and Electronic Documents Act* (Ottawa, May 2007). See recommendations 23–25.

1485 Industry Canada *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics – Statutory Review of the Personal Information Protection and Electronic Documents Act* (Ottawa, October 2007) 10.

1486 Jennifer Stoddart, Privacy Commissioner of Canada, to Richard Simpson, Industry Canada "Letter in response to Industry Canada's consultation regarding the review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)" (15 January 2008) Letter.

1487 Office of the Privacy Commissioner of Canada *Key Steps in Responding to Privacy Breaches* (Ottawa, 2007).

1488 The Privacy Act in Canada (R.S., 1985, c. P-21) only applies to public sector agencies. PIPEDA covers private organisations and businesses.

1489 It would be possible to sue on the tort of breach of privacy provided there is a "highly offensive" publication.

There is certainly little incentive to notify in cases where a breach would otherwise remain unknown to the affected individuals or public at large.[1490] There might also be insurance consequences: for example, companies might be reluctant to notify for fear of it being perceived as an admission of liability, thereby prejudicing rights to claim from their insurers. Proponents of breach notification argue that a mandatory notification requirement, backed up by adequate sanctions, is required to compel organisations to notify affected individuals in the absence of market based incentives to do otherwise. It has been stated that:[1491]

> A firm may not have an incentive to notify consumers of breaches when the cost of the notification exceeds the expected damage to the firm. That is, even if the costs of notifying a customer is smaller than the damage that will be mitigated, a firm has no incentive to bear this costs if the damage it will be spared is less than the costs of telling the customer... Second a firm may run the risk of damage as a result of notification.

Mandatory notification laws "level out the playing field" and make sure that considerations relating to insurance liability, and possible ramifications to a company's bottom line, do not encourage behaviour contrary to the public interest.

16.42 Mandatory laws are also said to provide the market with information about an organisation's information handling practices, making companies more transparent in the way they handle the information of customers and other individuals.[1492]

16.43 Such laws are also said to encourage firms to adopt and further secure safe document management practices, thereby "disinfecting"[1493] themselves of improper and unsafe security practices that are likely to result in personal information being compromised. Aside from a possible link between data breaches and data theft or fraud, it is not unreasonable to assume that mandatory laws provide some incentive for organisations to review their practices, given the negative publicity and consequences that can result after notifying about a breach. The negative publicity that can stem from data breaches is said to provide an incentive for organisations to encourage practices and processes that keep data secure. This point was central to the Australian Law Commission's reasoning in recommending the mandatory breach notification laws be introduced into the Australian Federal Privacy Act.[1494]

16.44 These benefits must be seen against some of the criticisms that are voiced in relation to mandatory breach notification laws. These include:

- the nominal effect that breach notification has been alleged to have had on reducing identity fraud;

1490 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 23.

1491 Michael Turner "Towards a Rational Personal Data Breach Notification Regime" (Information Policy Institute, 2006) 12.

1492 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.81.

1493 The term disinfectant relates to one of the rationales cited in support of data breach laws, "sunlight as disinfectant". See, for example, Sasha Romanosky, Rahul Telang, Alessandro Acquisti "Do Data Breach Disclosure Laws Reduce Identity Theft?" (Carnegie Mellon University, 2008) 2.

1494 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.73.

- the fact that, at least where there is a low threshold for notification, mandatory notification can lead to breach fatigue whereby the effectiveness of notices lessens as individuals are inundated by breach notifications; and
- the regulatory burden for public and private sector organisations and added costs that could be involved.

Q170 Should the Privacy Act include a mandatory breach notification requirement, or is a voluntary notification model more appropriate?

Substantive requirements

16.45 If a mandatory rules approach is adopted, developing the final notification package would need to involve consideration of the following factors.

Definition of data breach

16.46 In each US State the data breach laws prescribe the types of information that must be compromised before the obligation to notify arises. Specific definitions are required in the majority of cases in the absence of any generally applicable privacy law. Some guidelines, including those issued by the Office of the Privacy Commissioner, rely on the definition of personal information (or its equivalent) that exists in the privacy laws that support the guideline. In the New Zealand case, the guidelines relate to "personal information" as defined in the Privacy Act.[1495]

16.47 A data breach (or privacy breach as it is synonymously called) is defined in the New Zealand guidelines as "the result of unauthorised access to, or collection, use or disclosure of, personal information."[1496] Such activity is unauthorised if it occurs in contravention of the Privacy Act or its codes.[1497] This would include loss, theft, or mistaken disclosure.

16.48 The ALRC defined a data breach as a situation when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person.[1498] The ALRC recommended the adoption of a definition of "specified personal information" built on the definitions of "personal information" and "sensitive information" included in the Australian Privacy Act.[1499] The report recommends that the Act should prescribe the combinations of information that will constitute 'specified personal information' for the purposes of the notification regime. The report lists examples including driver's licence or proof of age; Medicare number or other unique identifier, such as tax file number; and sensitive information (as defined in the Australian Privacy Act). This combinational approach is also found in the California data breach

1495 Privacy Act 1993, s 2.

1496 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 1.

1497 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 2.

1498 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

1499 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

law (and the many US laws based on it).[1500] The ALRC made clear that any definition needs to cover more than sensitive financial information on the basis that financial harm "is not the only consequence that can flow from an unauthorised acquisition of personal information. Discrimination, stalking, and other harmful consequences potentially could flow from a security breach."[1501]

16.49 The Californian Statute defines personal information as "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: social security number, driver's licence number…, account number, credit or debit card number in combination with any security code…, medical information, and health insurance information."[1502] The definition excludes publicly available information that is lawfully made available to the general public from government records.[1503]

Q171 How should a data breach be defined? Should a data breach requirement be applicable to all types of personal information, or should a more purposive definition be developed for the purposes of the breach notification regime?

Notification threshold

16.50 One of the purposes of data breach notification is to give individuals an opportunity to mitigate any harm that could arise as a result of a data breach. The notification threshold that is set should balance the risks of breach-fatigue and undue stress to individuals with the benefit of giving individuals the opportunity to take steps when their personal information has been affected. Setting the threshold at a meaningful level can also avoid unnecessary stress and wasted time that an individual can expend as a consequence of a data breach notice. Setting the notification threshold at an appropriate level was "highlighted as the critical issue" for submitters to the ALRC's review of privacy.[1504]

16.51 The Canadian Internet Policy and Public Interest Clinic (CIPPIC) stated that "the trigger for notification should be based on a an objective test applied by organizations and subject to review by the applicable Privacy Commissioner. The test should be designed to avoid notification obligations where the breach does not expose individuals to a real risk of identity theft, but to apply in all situations where such a risk is created."[1505]

1500 California Civil Code § 1798.29 (e).

1501 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.98.

1502 California Civil Code § 1798.29(e).

1503 California Civil Code § 1798.29(f).

1504 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.48.

1505 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 25.

16.52 In California, the obligation to notify affected individuals is triggered when unencrypted personal computerised information "was, or is reasonably believed to have been, acquired by an unauthorized person."[1506] This is qualified in the case of good faith acquisitions made by employees in an organisation, provided that there is no further unauthorised disclosure.[1507] The standard required in California is known as the "acquisition standard" as no assessment needs to be made to consider whether there is any risk of the data being misused or compromised. The Californian standard sets the notification requirement threshold at a relatively low level. Even if an organisation believes that there is no risk at all to the individual concerned, it is still under an obligation to notify. It would for example, require notification in any case where an e-mail was sent to an unintended addressee, or where a USB key containing data was accidently disposed of. It is also of note that the Californian threshold is technology-specific in that it only relates to personal information that is computerised.

16.53 The ALRC recommended that the threshold for its notification regime be a *real risk of serious harm.*[1508] This is higher than the acquisition standard and requires the risk of harm to the affected person or persons be considered in deciding whether or not a notification should be made. The ALRC note that setting the trigger threshold at such a level should reduce the risk of breach fatigue and "also should reduce the compliance burden on agencies and organisations."[1509]

16.54 The New Zealand guidelines suggest that affected individuals be notified of 'material breaches' which requires considering whether harm could foreseeably result from the breach.[1510] In doing so, organisations are recommended to consider the sensitivity of the information, whether or not there is a risk that the information could be used in identity theft or fraud, and what harm (financial, physical, and personal/ reputational) could foreseeably result for the individual, the organisation and the public at large.[1511]

16.55 One model advanced by American commentators sets up a twin-track or split-threshold model where the level of risk of harm to the individual dictates who should be notified.[1512] Affected individuals will be notified only when there is a real risk that their personal information will be misused. In cases where there is a risk that information has been acquired, but nothing more, notification is only made to the regulatory body. This lower threshold would trigger the need to investigate further. The regulatory body will then audit the investigation

1506 California Civil Code § 1798.29 (a).

1507 California Civil Code § 1798. 29(d).

1508 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

1509 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.86.

1510 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 5.

1511 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 6.

1512 Paul M Schwartz and Edward J Janger "Notification of Data Security Breaches" (Online, 2007). Available online at www.paulschwartz.net/pdf/datasec_schwartz-janger.pdf (accessed 14 January 2010).

by the individual organisation and could step in if it believes an organisation erroneously decided not to notify. A similar dual notification model is reflected in the recommendations made by the CIPPIC.[1513]

Q172 In what circumstances should organisations be required to notify individuals that their personal information has been compromised? Should the legislation list the factors to be taken into account in deciding whether to notify? If so, what factors should the legislation list? Should there be different thresholds for notification to the individual and notification to the regulator?

The decision-maker

16.56 Both the model recommended by the ALRC[1514] and the New Zealand guidelines[1515] vest responsibility to decide whether a notification needs to be made with the organisation itself. This is also the case in all US States.[1516] Vesting the initial decision with the organisation enables it to develop its own standards and make judgements based on facts that it is most aware of. CIPPIC stated that the organisation itself should make the decision on the basis that it is in the best position to "calculate the associated risks of a breach of its information security".[1517]

16.57 The ALRC recommended that the decision reached by the organisation should be subject to oversight by the Privacy Commissioner who should be notified of data breaches that meet the threshold.[1518] The ALRC recommended that the decision to notify should be made in consultation with the Privacy Commissioner, and that the Privacy Commissioner should have the ultimate power to compel an organisation to notify if he or she believed, contrary to the view of the organisation, that the serious harm threshold was met.[1519] Notifying the Office of the Privacy Commissioner may be beneficial for agencies in terms of gaining further guidance concerning the breach and advice to ensure better practices in the future.[1520]

1513 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 26.

1514 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.87.

1515 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 6.

1516 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 17.

1517 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 26.

1518 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

1519 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.88.

1520 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 8.

16.58 In Canada, the House of Commons Standing Committee on Access to Information, Privacy and Ethics recommended that in the case of certain defined breaches of personal information, organisations should notify the Privacy Commissioner of the breach. The Committee recommended that upon being notified of a breach of personal information, the Privacy Commissioner must make a determination as to whether or not affected individuals and others should be notified, and if so in what manner.[1521] With this approach the decision to notify rests with the Privacy Commissioner. This recommendation was subsequently rejected.[1522]

16.59 Consideration should also be given to who should be required to notify in cases where data held by an affiliated third party, such as a contractor, is compromised. The Privacy Commissioner's guidelines suggest that it is usually appropriate for the organisation who has a direct link to the customer to notify but notes that there may be situations where it is a more appropriate task for the third party to do so.[1523]

Q173 Who should decide whether a notification must be made in response to a data breach?

Q174 Should the Privacy Commissioner have the power to compel an organisation to notify affected individuals?

Who to notify

16.60 The New Zealand guidelines, the US data breach laws, and the recommendations made by the ALRC all mandate notifying individuals whose personal information is compromised. The benefits of notifying individuals in these cases have previously been canvassed in the chapter.

16.61 It is also timely to consider whether the Privacy Commissioner or other interested parties should be notified, and if so at what stage in the process. In relation to the Privacy Commissioner, this decision will need to be made in light of the response to the policy question above – that which asks who should make the decision to notify. If it is the Privacy Commissioner, then their office will necessarily be contacted in each case. However, even if the decision is to be made by the agency itself, there may still be some merit in advising the Privacy Commissioner in each case, both for the agency concerned (for example in terms of guidance) and for policy development in the area (including trying to understand the extent of the problem).

1521 House of Commons Standing Committee on Access to Information, Privacy and Ethics (Can) *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics – Statutory Review of the Personal Information Protection and Electronic Documents Act* (Ottawa, May 2007) 45.

1522 This recommendation was subsequently rejected by the Canadian Government in its official response, on the basis that the organisation itself would be well positioned to understand and assess the risks involved with notification. See *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA), Fourth Report* (Ottawa, October 2007).

1523 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 7.

16.62 It would also be possible to include a requirement that, in certain cases, agencies notify other interested parties. Such parties could include financial regulatory bodies, credit card companies, insurers, organisations on behalf of whom the information was held, or law enforcement agencies such as the police.

16.63 Notifying credit card companies could ensure action is taken to monitor accounts and be on notice of suspect behaviour. The benefits of notifying particular bodies would differ from case to case.

Q175 In the case of a data breach should the agency be required to notify the Privacy Commissioner's Office? If so, should this be in every case, or only when the "notification threshold" is met?

Q176 Should other agencies be notified? If so, in what circumstances?

Process requirements

Timing

16.64 In its white paper on data breach laws, CIPPIC suggests that:[1524]

> Security breach notification should be undertaken as soon as possible and without unreasonable delay after the occurrence of the breach, except where a law enforcement agency has made a written request for a delay. Delays for law enforcement purposes should be specified periods of time, and for not longer than 60 days at a time.

16.65 The New Zealand guidelines suggest notification should occur as soon as reasonably possible following assessment and evaluation of the breach and includes a similar extension provision for law enforcement purposes.

Q177 At which point should notification be required?

Q178 Should delays in notifying be allowed for law enforcement or any other purposes?

Method of notification

16.66 The CIPPIC paper recommends that notification should "generally be by regular mail, but electronic and substitute notice should be permitted when certain conditions are met."[1525]

1524 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 18.

1525 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 28.

16.67 The New Zealand guidelines are similar. Notification should be direct – by phone, letter, email or in person. Substituted notification is provided for in cases where an individual's contact details are unknown, or where a particularly large number of individuals are affected and direct contact would result in further harm or is prohibitive in cost for the organisation. Multiple methods of notification are also included as an option.[1526] In California substituted service is allowed if the cost of notification would be over US$250,000, or where the number of affected people exceeds 500,000.[1527]

Q179 Should the method of notification be prescribed, or stated in terms of the objective to be achieved?

Content of the notification

16.68 For notifications to be meaningful, and provide individuals with the ability to reduce the adverse effects that can flow from data breaches, sufficient information for the individual to act upon must be included in the notification. The New Zealand guidelines suggest that the following be included:[1528]

- information about the incident and its timing in general terms;
- a description of the personal information involved in the breach;
- a general account of what the agency has done to control or reduce any harm;
- what the agency will do to assist individuals and what steps an individual can take to mitigate any harm, including directing individuals to further information;
- contact information of a person or department within the agency who can provide further information;
- sources of further information such as the Police, the Ministry of Consumer Affairs, or Netsafe;
- whether the organisation has notified the Office of the Privacy Commissioner; and
- the contact information of the Privacy Commissioner.

Q180 What information should have to be included in a breach notification?

Exceptions

16.69 In some US States specific exceptions exist that remove the requirement to notify in a particular case, thereby recognising that in certain cases other rights trump the important right to know that information has been compromised. Some of these considerations could be dealt with as a factor to weigh up when considering the level of risk of harm to the individual (such as encryption). Alternatively, some interests (such as state security) may be absolute exceptions.

16.70 Specific exceptions are discussed below.

1526 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 7.

1527 California Civil Code § 1798. 29(g)(3).

1528 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 7.

Encryption

16.71 Some US States treat the encryption of data as a specific exception from the obligation to notify on the basis that the likelihood of harm resulting from a breach involving encrypted data is small. Other models deal with encryption as part of the risk assessment exercise that is carried out when making a decision whether or not to notify. The ALRC took the latter approach.[1529]

16.72 The ALRC acknowledged that encryption should be a ground to excuse an organisation from the obligation to notify but noted that any encryption must be "adequate". This recognises the different data encryption techniques that exist and the difficulty of comparing them. An assessment of whether or not encryption is "adequate" will depend on the particular facts of the case.[1530] The ALRC recommends that the Privacy Commissioner issue guidance as to what forms of encryption are "adequate" for the storage of personal information.

Public interest exception

16.73 In response to the concerns of stakeholders to its review, the ALRC recommended that the Privacy Commissioner should have a broad discretion to waive the notification requirement when notification would not be in the public interest.[1531] This decision would lie with the Privacy Commissioner. This could apply in cases such as where the information involved concerns matters of national security.

Other exceptions

16.74 Other express exceptions could be included in the breach notification regime to ensure that certain important interests are adequately protected.

Q181 What exceptions, if any, should be included in a data breach notification regime? In particular:

- Should encryption be an express exception or one of the matters to be included in the risk assessment exercise?
- Should public interest be included as a ground on which the Privacy Commissioner can waive an organisation's obligation to notify, or are more narrowly-defined exceptions more appropriate?

Failures to notify

16.75 Rules are generally meaningless without the availability of sanctions in cases where they are not followed. If a mandatory rule approach is adopted it is important to consider what sanctions are available in situations where an organisation fails to notify individuals affected by a data breach. An individual would have recourse through making a complaint to the Privacy Commissioner, either on the basis

1529 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.91.

1530 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.92.

1531 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.94.

of a new ground of complaint (a failure to notify) or under existing grounds such as a failure to take reasonable steps to protect personal information (under principle 5).

16.76 The complaint could be dealt with in accordance with the options we are proposing in chapter 8. If the Privacy Commissioner found that an agency was in breach of the terms of the Act, if the proposals are adopted, he or she would then have the ability to issue an enforcement notice. Essentially an enforcement notice is a notice to comply with the terms of the Privacy Act issued by the Privacy Commissioner that carries consequences for failing to comply.[1532]

Q182 Is the complaints process an adequate mechanism for dealing with an organisation's failure to notify in the case of a data breach, or are further sanctions necessary?

Vehicle for a mandatory model

16.77 If a mandatory notification requirement is to be adopted, consideration needs to be given to how it would be introduced into the Privacy Act regime. Our tentative opinion is that if a notification requirement were to be mandated, it should be enacted as an aspect of one of the privacy principles, with corresponding detailed provisions inserted in a new part or sub-part later in the Act.

16.78 As noted above, in investigating a complaint concerning a breach of principle 5, the Privacy Commissioner currently takes into account the failure to notify individuals whose information has been compromised in appropriate cases. This must be because notification can be considered a security safeguard that agencies should use to protect the personal information that they hold. The Law Commission believes that it would be possible to add a new sub-paragraph (c) to principle 5 that contains the notification obligation. We also envisage that this could contain a cross-reference to sections or a part later in the Act, as is the case with Principle 6(3), and that those later sections or later part can include the more detailed requirements that collectively make up the notification scheme.

16.79 We also wish to point out that codes could be used to tailor aspects of technical reporting requirements or varying requirements to particular sectors or contexts. We have no view on the need for particular codes at this time but foresee codes as an appropriate means to tailor requirements where necessary.

Q183 Should it be decided that notification should be mandatory, do you agree that an amendment to principle 5, backed up by provisions later in the Act, is the best way to enact an obligation to notify? If not, how do you think the obligation should be enacted?

1532 Enforcement notices are proposed and discussed in more detail in chapter 8.

Chapter 17
Identity crime

17.1 This chapter discusses the problem of identity crime, and whether the Privacy Act might be able to do more to assist in protecting against it.

WHAT IS IDENTITY CRIME?

Definitions

17.2 There is no universally accepted definition of identity crime, which is often also called identity fraud or identity theft. This chapter is about identity crime in its broadest sense, so we use all three terms.

17.3 The Australian Centre for Policing Research has developed the following definitions:[1533]

> **Identity crime** is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of a crime.
>
> **Identity fraud** is the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity.
>
> **Identity theft** is the theft or assumption of a pre-existing identity (or a significant part thereof), with or without consent, and whether, in the case of an individual, the person is living or deceased.

17.4 The New Zealand Police describe identity crime as any offence involving the misuse of identity. They do not include traditional theft and misuse of credit cards or cheques in either the description or the statistics of identity crimes, as these are already well established and understood. In contrast, other jurisdictions such as the United States do treat such offences as identity crime.

17.5 As noted above, offenders use 'identities' in a variety of ways. Police currently estimate that misuse of a genuine identity makes up about half of identity crime. This includes offenders using their own identity, or variations such as changes

1533 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General *Final Report: Identity Crime* (Canberra, 2008) 8.

of name. About a quarter of cases involve the use of fictional identities and the remaining quarter involves the unauthorised use of another identity. This includes the misuse of identities of deceased people.[1534]

17.6 Once obtained, offenders use identities for a wide variety of unlawful activities. Some of the most common include misuse of existing accounts (for example, gaining access to a victim's bank account and stealing money), opening new accounts, obtaining credit (for example, obtaining a loan in a victim's name, using the loaned money to make purchases and then defaulting on the loan), and fraudulently obtaining government benefits, services or documents. Offenders also use identities to avoid detection or avoid meeting obligations (such as child support payments). Identity theft for the purpose of obtaining health care is a problem in the US.[1535] A further problem is unauthorised brokering of personal information.

How identity crime is committed[1536]

17.7 Identity crime can be committed using a wide variety of techniques. While it is not a new phenomenon, the development of technology, particularly the internet, has enabled the development of many new techniques and made identity crime more prevalent. Establishing one's real identity for online transactions is more complex than in a face-to-face transaction, making fraud easier. This section describes some of the key ways in which identity crime is committed. It should be noted, however, that the techniques are evolving and transforming into new types of threats very rapidly.

Phishing

17.8 Phishing involves the use of deceptive emails or mirror websites, which look like the websites of legitimate businesses, to get users to provide personal information. A common example is an email pretending to be from a bank, asking customers to provide their account details. Phishing messages are commonly distributed through unsolicited emails (spam), and can also be used to install malware (see below) on the computers of recipients.

17.9 Phishing can take many forms, and is now often used in conjunction with malware. The techniques are becoming increasingly sophisticated and harder to detect. Some key forms include:

- "Pharming": using deceptive emails to redirect users from an authentic website to a fraudulent one, which replicates the original site.

1534 New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008) 66. We note that there are several government information matches in place that use deaths information to discover misuse of identity information.

1535 Kristen Gerencher "Preying on Patients" (24 June 2008) *The Wall Street Journal* United States.

1536 Unless otherwise noted, information in this section is taken from Organisation for Economic Cooperation and Development *Online Identity Theft* (OECD Publishing, Paris, 2009) 3.

- "SMisShing": sending text messages to cellphone users that trick them into going to a website operated by the offenders. Messages often say that unless recipients go to the website to cancel, they will be charged for services that they never ordered.
- "Vishing": this technique uses Voice over Internet Protocol to steal personal information through a telephone. Victims typically receive an email disguised as one from a legitimate business, which invites the recipient to call a telephone number and give out personal information for security purposes.
- "Spear-phishing": impersonating a company employee via email in order to steal colleagues' passwords or usernames and gain access to the company's computer system.

Malware

17.10 Malware refers to malicious software that is surreptitiously installed into a computer or device (such as a cellphone) to collect the user's personal information over time. Types of malware include:[1537]

- keystroke loggers: programmes that record how a keyboard is used;
- rootkit: a set of programmes designed to conceal the fact that a computer has been compromised at the most privileged base or "root" level; and
- Trojan horses: programmes that appear legitimate but which actually have hidden functionality used to circumvent security measures and carry out attacks.

As noted above, unsolicited messages are often used to load malware onto recipients' computers.

Social engineering

17.11 Social engineering is a broad term describing practices that rely on a victim providing personal information to another person, either in person or over the telephone or internet.[1538] Deception or trickery is often involved. Some of the practices include:

- "Pretexting": this involves using an invented scenario in order to persuade a target to release information. Pretexters often contact a company, usually a financial institution, impersonating a legitimate customer, and request their account information. In other cases, the pretext is accomplished by an insider at the institution or by fraudulently opening an online account in a customer's name.
- "Shoulder surfing": this involves eavesdropping on public transactions to obtain personal information or looking over a victim's shoulder, or watching from a nearby location, as they enter their PIN.

Social networking

17.12 Offenders are increasingly using social networking sites to commit identity crime. Due to the amount of personal information posted on social networking sites, identity thieves often gather details about victims which they then use to,

1537 Organisation for Economic Cooperation and Development Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy *OECD Policy Guidance on Online Identity Theft* (Paris, 2008) Appendix H.3.

1538 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 12.6.

for example, hack into bank accounts. In one example, hackers broke into a woman's Facebook account and sent a message to all her friends saying that she had been assaulted and robbed in London and urgently needed money to get home. The message asked recipients to wire money to a Western Union account.[1539]

Other

17.13 Other common methods used to commit identity crime include:

- stealing personal information from computer databases;
- consumer scams used to gather personal information;
- stealing mail;
- searching rubbish bins to obtain discarded items containing personal information, such as credit card or bank statements (sometimes referred to as "dumpster diving"); and
- credit card skimming, which involves recording personal data from magnetic strips on the back of credit cards, the data then being transmitted to another location where it is re-encoded onto fraudulently made credit cards.

EFFECTS OF IDENTITY CRIME

Effects on victims

Financial loss

17.14 Identity crime often causes direct or indirect financial losses for victims. This may include loss of savings, credit card, loan or utility bills incurred in the victim's name, and damage to credit rating.

Psychological and social impact

17.15 Identity crime harms a victim's privacy and sense of individuality. It can cause trauma and stress, and victims may become less likely to participate in society.[1540] Victims may also feel unsafe if offenders have discovered information such as their address that could lead to a physical threat.

Damage to reputation

17.16 At the most serious end of the scale, victims may be convicted of crimes they did not commit. Probably the most common form of damage to reputation is victims having negative information placed on their credit reports. The flow-on effects of this reputational damage can be significant. For example, victims might later be denied loans or housing as a result of negative information on their credit reports.

17.17 The time and effort required for victims to restore their reputation can often be very significant. One estimate is that around a third of victims spend 40 hours or more resolving problems and clearing their name. In cases where there has

1539 Asher Moses "Robbed on Facebook – one victim's story" (9 September 2009) *Sydney Morning Herald* Sydney.

1540 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General *Final Report: Identity Crime* (Canberra, 2008) 5.

been a "total hijack" (where the victim's identity information has been used numerous times to defraud multiple organisations) victims may spend over 200 hours and up to £8000.[1541]

Effects on society

Law and order and national security

17.18 Identity crime facilitates other crimes. In most cases, offenders engage in identity crime with a view to committing further crimes, such as stealing money, obtaining credit, or obtaining social welfare benefits. There is evidence that identity crime is increasingly being used by organised crime groups for activities such as people trafficking or smuggling. The hijackers involved in the 11 September 2001 terrorist attacks in the United States used false identities and fraudulent social security numbers and identification documents to facilitate their crimes. Terrorist networks have often used false identity documents to obtain employment overseas, finance their activities and avoid detection.[1542]

Costs to the economy

17.19 Costs to the economy resulting from identity crime include the costs associated with preventing, detecting and responding to identity fraud as well as direct losses resulting from it. By way of example, in Australia estimates of the cost of identity crime in 2007 range from US$1 billion to over US$3 billion.[1543] At the 2008 G8 ministers' meeting in Tokyo, it was estimated that identity crime cost the USA $66 billion and Europe over $130 billion in 2007.[1544] Similar estimates for New Zealand are not available, but it seems reasonable to assume that identity crime similarly represents a large cost to our economy.

17.20 Agencies' reputations are likely to be damaged if personal information they hold is used to commit identity crime. Businesses may lose customers and citizens are less likely to trust government agencies that have not held their personal information securely.[1545]

17.21 There is also evidence that risks associated with transacting in an online environment, including the risk of identity crime, can act as a barrier to the expansion of e-commerce.[1546]

1541 Organisation for Economic Cooperation and Development Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy *Scoping Paper on Online Identity Theft* (Paris, 2008) 31.

1542 F Paget *Identity Theft White Paper* (2007), cited in Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General *Final Report: Identity Crime* (Canberra, 2008) 5.

1543 Organisation for Economic Cooperation and Development *Online Identity Theft* (OECD Publishing, Paris, 2009) 37.

1544 Cliff Taylor "Identity theft on the rise" (15 June 2008) *New Zealand Herald* Auckland.

1545 Department of Internal Affairs *Evidence of Identity Standard Version 1.9 (Draft)* (Wellington, 2009) 41.

1546 Organisation for Economic Cooperation and Development *Online Identity Theft* (OECD Publishing, Paris, 2009) 18.

WHAT IS THE EXTENT OF THE PROBLEM IN NEW ZEALAND?

17.22 It is difficult to get an accurate picture of the extent of identity crime in New Zealand, because it is reported as different offences (we discuss the offences below). In the 12 months to June 2008 there were 900 cases detected.[1547] However, Police believe that identity crime is widespread. It is probably under-reported and a lot goes undetected.

17.23 Overseas studies have found that the incidence, extent and cost of identity crime are increasing in a number of countries, including Australia,[1548] although recently it appears to be declining somewhat in the USA.[1549] It seems reasonable to assume that overseas trends are reflected in the incidence of identity crime in New Zealand.

17.24 A 2002 study of 361 Australian and New Zealand public and private sector organisations found an increase in the involvement of criminal gangs in fraudulent attacks on financial institutions by using falsified identification and stolen cheques. International criminals were also increasingly coming into Australia and New Zealand, committing fraud and then leaving with the proceeds.[1550]

CURRENT LAW

17.25 New Zealand law contains a number of provisions that can be used to address aspects of identity crime, although there is no law specifically targeted at identity crime. We outline the current law below.

Criminal law

17.26 There are a number of criminal offences that can be used to prosecute identity crime, depending on the circumstances of particular cases. Offences under the Crimes Act 1961 are:

- section 219, theft or stealing;
- section 228, dishonestly taking or using a document;
- section 240, obtaining by deception or causing loss by deception;
- section 249, accessing a computer system for a dishonest purpose;
- section 251, making, selling, distributing or possessing software for committing crime;
- section 252, accessing a computer system without authorisation;
- section 256, forgery;
- section 257, using forged documents; and
- section 258, altering, concealing, destroying or reproducing documents with intent to deceive.

1547 Cliff Taylor "Identity theft on the rise" (15 June 2008) *New Zealand Herald* Auckland.

1548 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General *Final Report: Identity Crime* (Canberra, 2008) 9. See also United Nations Economic and Social Council, Commission on Crime Prevention and Criminal Justice "Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity" (31 January 2007) E/CN.15/2007/8/Add.3, para 27: most states reported that identity crime is increasing, and a very rapid increase was noted in several states.

1549 Fred Cate *Information Security Breaches: Looking back & thinking ahead* (Centre for Information Policy Leadership, 2008).

1550 Caslon Analytics *Identity Crime Statistics* www.caslon.com.au/idcrimeguide12.htm (accessed 9 September 2009).

17.27 Relevant offences under other Acts include:

- Summary Offences Act 1981, section 19, imitation of official documents; and
- Social Security Act 1964, section 127, making a false or misleading statement to obtain a benefit.

Privacy law

17.28 Identity theft is a potential consequence of an interference with the privacy of an individual. As such, the Privacy Act and other privacy laws are only indirectly relevant to identity crime: they mandate good information handling practices that can help to prevent identity crime, and can help to minimise the harm caused by identity crime after it has occurred.

Information Privacy Principles

17.29 All the principles play a role in dealing with identity crime:

- Principle 1 helps to limit the amount of personal information collected by agencies, thereby limiting the information that can be accessed for identity crime purposes.
- Principles 2 and 3 help to give individuals control over their information, and to ensure that they should usually know who holds it and the purposes for which it may legitimately be used. This makes it easier for them to know who to go to if their identity is misused.
- Principle 4 deals with situations in which identity thieves use unlawful or unfair means to obtain personal information.
- Principle 5 helps to ensure that personal information is protected by reasonable security safeguards.
- Principles 6 and 7 allow people to monitor and correct information that is held about them, which helps with both detecting and combating identity crime.
- Principle 8 ensures that the accuracy of personal information is checked before it is used.
- Principle 9, like Principle 1, limits the amount of personal information that agencies hold, and therefore the amount of information that can be obtained by criminals.
- Principle 10 means that use of a person's identity for a purpose other than the one for which the identifying information was collected will be a breach of this principle.
- Principle 11 limits disclosure of personal information, which makes it more difficult for personal information to be obtained and then used to commit identity crime.
- Principle 12 controls the use of unique identifiers. Without controls on their use, unique identifiers can be a powerful tool in the hands of identity thieves, allowing them easily to link different aspects of a person's identity. Social Security Numbers in the US have been widely used in this way.

17.30 While principle 6 can allow people to monitor and correct information held about them, it can also make personal information vulnerable to misuse. A person masquerading as the individual concerned may obtain access to personal information which can be used to commit identity theft. The Act

does contain some protections against this practice: section 45 requires agencies to take precautions to establish the identity of the person making the request before giving access. We discuss whether so-called "pretexting" should be an offence in chapter 8.

Public Register Privacy Principles

17.31 Public registers are a common source of personal information which is then used to commit identity crime. Thus, the Public Register Privacy Principles have a part to play. The most relevant is Public Register Privacy Principle 2, which requires that personal information from a public register shall not be resorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

17.32 There have been moves to restrict access to public registers, such as the register of births, deaths and marriages and the motor vehicle register, to reduce the risk of identity crime that open access to public registers can pose. In the Law Commission's report for stage 2 of this review, we recommended changes to the law governing public registers.[1551]

Information matching

17.33 As we have discussed in chapter 9, the Act regulates government information matching. Information matching is often used to detect identity fraud, such as the use of multiple identities or of identities of deceased people.

Credit Reporting Privacy Code 2004

17.34 Credit reporting is relevant to identity crime in a number of ways. Those committing identity crimes often obtain credit in other people's names. Improper access to credit reporting information also represents a risk. On the other hand, the credit reporting system can also be used to prevent or detect identity crime. For example, credit monitoring helps people to detect improper use of their identities to obtain credit.

17.35 The Privacy Commissioner sees the Credit Reporting Privacy Code as an important protection against identity crime. The code places a high value on improving the accuracy of credit reporting, and limits the secondary uses of credit information, reducing the opportunities for misuse.[1552] It requires credit reporters to:[1553]

- provide individuals with free copies of any information held about them;
- regularly update credit information;
- have systems to ensure new information is linked to the correct individual;
- have systems and audits to ensure information is accurate;

1551 New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008).

1552 Office of the Privacy Commissioner *General Information Paper* www.privacy.org.nz/general-information-paper (accessed 9 September 2009).

1553 See Office of the Privacy Commissioner www.privacy.org.nz/credit-reporting-privacy-code (accessed 9 September 2009).

- flag disputed debts while they are being checked;
- limit the range of agencies and individuals to which credit information can be disclosed; and
- have clear, fast and effective complaints resolution procedures.

17.36 The requirement to provide free copies of credit information is important, as it allows people to check their credit report regularly and to seek correction of any inaccuracies. Victims may not always be aware that identity crime has occurred, and only discover it later when they are refused credit due to the actions of identity thieves in their name. Providing free copies of credit information helps to detect cases of unauthorised access or evidence of identity crime.

17.37 The Commissioner is currently reviewing the Code and will consider amendments, such as posting alerts or "freezing" files, which may provide better protection against identity crime.

Other

Financial Transactions Reporting Act 1996

17.38 Part 2 of this Act contains obligations on financial institutions to verify the identity of people wanting to become facility holders, people conducting certain occasional transactions and people acting on their behalf. Identity can be verified via documentary evidence or any other evidence capable of establishing identity. It is an offence to contravene these requirements.[1554]

Unsolicited Electronic Messages Act 2007

17.39 As described above, unsolicited electronic messages are often used as a mechanism for committing identity crime. The Unsolicited Electronic Messages Act is designed to reduce spam, and thus helps to fight identity crime. The Act's key requirements are that unsolicited messages must not be sent, commercial messages must include accurate information about their sender and a functional unsubscribe facility. Address-harvesting software or address-harvested lists must not be used to send unsolicited messages.

Code of Banking Practice of the New Zealand Bankers' Association

17.40 The Code of Banking Practice of the New Zealand Bankers' Association, of which the majority of banks are members, contains a number of provisions directed at helping to reduce banking fraud. The Banking Ombudsman considers complaints about breaches of the Code. Especially relevant are the provisions on internet banking. Banks must take appropriate measures to ensure that their systems and technology are secure. They also undertake to provide customers with information about how to protect themselves against fraud, and never to send emails asking customers to confirm their information or disclose passwords by email. Banks will reimburse customers who suffer direct losses

1554 Financial Transactions Reporting Act 1996, s 13.

as a result of a security breach, provided that there was no negligence on the customer's part (such as choosing a password of a type that they had been warned not to use).[1555]

Tort law

17.41 The tort of deceit involves a false representation as to a past or existing fact made by a defendant who knew it to be untrue or who had no belief in its truth or who was reckless as to its truth; intention that the plaintiff should have acted on the representation; and action by the plaintiff in reliance on the representation. The plaintiff must suffer damage as a result of relying on the representation.[1556] Cases of identity crime often may satisfy these requirements, so victims could take court action to seek redress from the perpetrators.

Payment Card Industry Data Security Standard

17.42 The Payment Card Industry Security Standards Council has developed an industry standard, which applies to credit card companies worldwide. It requires security measures such as encryption of transmissions of cardholder information, protection of credit card information on websites and truncation of credit card numbers on receipts.

INTERNATIONAL LANDSCAPE

17.43 Overseas developments seem to indicate a growing trend towards enacting specific laws, especially criminal laws, targeting identity crime. This section outlines overseas developments of interest, especially in countries comparable to New Zealand.

Australia

17.44 At Federal level, there are numerous general offences that can be used to prosecute identity crime. In addition, the Model Criminal Code Law Officers' Committee has recommended the creation of three identity crime model offences, relating to dealing in identification information, possession of identification information with the intention of committing an indictable offence, and possession of equipment to create identification information. There should also be provision for local courts to issue a certificate to a victim of identity crime if satisfied on the balance of probabilities that one of the above offences has been committed, with the intent that the certificate may assist with any problems the offence has caused in relation to the victim's personal or business affairs.[1557] At the time of writing, the Standing Committee of Attorneys-General had agreed to prepare a review paper examining implementation priorities for the report.[1558]

17.45 In the majority of states, identity crime is dealt with through the general criminal law. However, specific identity crime offences have been enacted in South Australia and Queensland. In South Australia it is an offence to assume the

1555 New Zealand Bankers' Association www.nzba.org (accessed 14 September 2009).

1556 *Amaltal Corporation Ltd v Maruha Corporation* [2007] 1 NZLR 608, paras 46 and 55 (CA), cited in Stephen Todd (ed) *The Law of Torts in New Zealand* (5th ed, Brookers, Wellington, 2009) 707.

1557 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General *Final Report: Identity Crime* (Canberra, 2008) 25–27.

1558 Standing Committee of Attorneys-General "Communiqué" (28 March 2008) Media Release.

identity of another person (whether living or dead, real or fictitious, natural or corporate) with the intent to commit, or facilitate the commission of, a serious criminal offence, which is defined as an indictable offence or an offence prescribed by regulation.[1559] It is also an offence to use the personal identifying information of a living or deceased person, or a body corporate, with the intent to commit, or facilitate the commission of, a serious criminal offence.[1560] Queensland has similarly enacted an offence of obtaining or dealing in identification information for the purpose of committing, or facilitating the commission of, an indictable offence. It is immaterial whether the victim is living or dead, real or fictitious. The Act also provides for the court to issue a certificate to the victim.[1561]

USA

17.46 There has been significant legislative activity to address identity crime in the USA. It is worth noting that the US has no comprehensive data protection law, which may partially explain the need for specific legislation on identity crime.[1562]

17.47 At federal level, key pieces of legislation are the Identity Theft and Assumption Deterrence Act of 1998 and Identity Theft Penalty Enhancement Act of 2004, making it an offence punishable by up to 15 years' imprisonment or a fine of US$250,000 to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, aid or abet any unlawful activity.

17.48 The Identity Theft Enforcement and Restitution Act of 2008 made it easier for prosecutors to prosecute cybercrime, by removing a requirement that there be at least $5000 in damages before charges for unauthorised access to a computer could be brought. It also aimed to ensure that victims are compensated for their time and trouble. In cases where convicted identity thieves are ordered to pay restitution, the victim must receive a portion of the money "equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offence."[1563]

17.49 The US has also enacted legislation relating to credit reporting. The Fair and Accurate Credit Transactions Act 2003 introduced protections for consumers, including that they must be able to obtain a free credit report on request, and be able to place a fraud alert on their account. Once an alert has been placed, credit reporting agencies must block potentially fraudulent information on credit reports from being released.

17.50 The Federal Trade Commission began enforcing the "red flags rule" in May 2009. This rule requires financial institutions and creditors (including finance companies, mortgage brokers, real estate agents, automobile dealers, and retailers that offer financing or help consumers to get financing from others) to implement a written

1559 Criminal Law Consolidation Act 1935 (SA), s 144B.

1560 Criminal Law Consolidation Act 1935 (SA), s 144C.

1561 Criminal Code Act 1899 (Qld), s 408D.

1562 For more information about US privacy legislation, see New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2008) para 4.26.

1563 See further Brian Krebs "New Federal Law targets ID Theft, Cybercrime" (1 October 2008) *Washington Post* Washington, DC.

Identity Theft Prevention Program designed to detect the warning signs ("red flags") of identity theft in their operations, take steps to prevent it, and mitigate the damage if it does occur.[1564]

17.51 Many states also have their own legislation about identity theft. Identity theft is an offence in the majority of states.

Canada

17.52 Canada has recently created three new offences: obtaining and possessing identity information with the intent to use the information deceptively, dishonestly or fraudulently in the commission of a crime; trafficking in identity information and unlawfully possessing or trafficking in government-issued identity documents. All carry maximum penalties of five years' imprisonment. Police now have clearer powers to act upon finding identity information, so that they can prevent use of the information to commit crime. The law also allows for an order that the offender make restitution to a victim of identity theft or identity fraud for the expenses associated with rehabilitating their identity.[1565]

UK

17.53 While the UK does not have comprehensive identity crime offences, it does have some offences targeting aspects of identity crime. It is an offence, with some exceptions, to obtain, disclose or procure the disclosure of personal data without the consent of the data controller.[1566] This provision could be used to prosecute some cases of identity crime. It is also an offence to possess or control false identity documents, including genuine documents that have been improperly obtained or were issued to another person, without reasonable cause. This covers both UK and foreign identity documents.[1567]

South Korea

17.54 The South Korean government made it mandatory in 2006 for financial institutions to compensate customers who are victims of online fraud and identity theft. Customers are not entitled to compensation if they are careless with their data.[1568]

ARE ANY LAW CHANGES NEEDED?

17.55 In this chapter we have outlined the ways in which existing law can be used to prevent and punish identity crime, and to minimise the harm that it causes. We would like to hear submitters' view on whether the current law is sufficient, or whether more should be done.

1564 Federal Trade Commission *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business* www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.shtm (accessed 24 August 2009).

1565 An Act to amend the Criminal Code (identity theft and related misconduct) 2009.

1566 Data Protection Act 1998 (UK), s 55.

1567 Identity Cards Act 2006 (UK), s 25.

1568 Electronic Financial Transactions Act 2006 (South Korea). See also "Korean Banks forced to compensate hacking victims" www.finextra.com (accessed 15 September 2009).

17.56 In chapter 16 we discuss whether the Act ought to require data breach notification. Data breach notification may help to reduce identity crime,[1569] in that people whose personal information has been exposed are made aware that they may be at risk of identity theft and can then take steps to protect themselves. This is perhaps the most likely change that could be made to the Act to further address identity crime.

17.57 The Privacy Commissioner has recommended that consideration be given to the merit of including controls in principle 12 to encourage number truncation or other ways of controlling the public display of unique identifiers.[1570] This could be of some assistance in preventing identity crime because identity thieves can discover a lot of personal information about someone if they obtain a unique identifier relating to them. Unique identifiers can be publicly displayed by, for example, printing them on documentation (such as invoices displaying the credit card number used to make a purchase). Controlling the public display of unique identifiers would make it more difficult for identity thieves. One way of doing this might be through number truncation, where only some numbers comprising a unique identifier are displayed and the rest are blanked out.[1571]

17.58 We are interested in submissions on the above points, and whether there could be any further changes to the Act that would help to prevent identity crime or reduce the harm once it has occurred. In addition, should there be specific identity crime offences, as have been enacted in some jurisdictions?

Q184 Are any changes needed, either to the Privacy Act or to other laws, to better address identity crime?

1569 We note, however, that the evidence that it has had this effect in the US is not strong.

1570 *4th supplement to Necessary and Desirable* recommendation 28A.

1571 *4th supplement to Necessary and Desirable* para 2.7

Chapter 18
Particular groups

18.1 For the most part, the Privacy Act applies in the same way to everyone. This chapter considers whether there are any ways in which special provision needs to be made within the framework of the Privacy Act for particular groups in society. We consider in particular cultural groups (especially Māori), children and young people, and adults with reduced capacity.

CULTURE AND PRIVACY

18.2 In our study paper for stage 1 of this Review, we gave some consideration to the fact that, while a desire for some form of privacy appears to be universal among human beings, the ways in which privacy is understood may differ between cultures.[1572] We also looked more specifically at Māori understandings of privacy, and explored in a preliminary way some issues relating to Māori and privacy.[1573] We noted, among other things, that opinion surveys indicate a degree of divergence between Māori and non-Māori on some privacy issues.[1574]

18.3 There are legislative precedents for making special provision for information of particular concern to Māori. The Local Government Official Information and Meetings Act 1987 provides that certain types of information requested under the Act may be withheld if necessary "to avoid serious offence to tikanga Māori, or to avoid the disclosure of the location of waahi tapu".[1575] The Health (Cervical Screening (Kaitiaki)) Regulations 1995 provide for the establishment of a National Kaitiaki Group to consider, and approve when appropriate, applications for approval to disclose, use or publish information on the National Cervical Screening Register that identifies women as being Māori. The Regulations specify the matters that the Group shall have regard to in considering such applications.[1576]

1572 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 102–104.

1573 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 104–108.

1574 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 117–118.

1575 Local Government Official Information and Meetings Act 1987, s 7(2)(ba).

1576 Health (Cervical Screening (Kaitiaki)) Regulations 1995, reg 5(3). Although not established under specific regulations, there is also a Pacific Women's Data Advisory Group which considers applications for the release of Pacific women's aggregated data from the National Cervical Screening Register. See "National Kaitiaki Group" and "Pacific Women's Data Advisory Group" on the website of the National Screening Unit, www.nsu.govt.nz (accessed 3 December 2009).

18.4 At this stage, we do not propose that the Privacy Act should be amended to make provision for information that is specific to Māori or any other ethnic, religious or cultural group. We do, however, think it is worth exploring whether there are any ways in which either the provisions or the application of the Privacy Act can be made more relevant to a culturally-diverse society.

Māori

18.5 In June 2008, the Law Commission held a meeting with a group of Māori from a range of backgrounds to discuss privacy issues that affect Māori. The key issues from that discussion are summarised below. Issues for Māori relating to privacy and the media are discussed in our report for stage 3 of this Review.[1577]

Collective and individual privacy

18.6 The Commission was told that Western concepts of privacy focus on the individual, whereas Māori are more likely to focus on collective interests. For example, in the health field information is generally managed on an individual basis, but some Māori may feel that information about a person's health belongs not only to the individual but also to that person's whānau, hapū or iwi. This can lead to tensions between the individual and the collective, but also to conflict within groups when people have different ideas about the use of information. On the other hand, it was stressed to the Commission that individual privacy is connected to the collective, so that individual and collective privacy interests may be mutually reinforcing. We were told that privacy is based on respect for individual human dignity, which is also a fundamental value in Māori culture. An idea of privacy based on respect for dignity and autonomy should also be able to accommodate collective rights and interests.

Trust and uses of information

18.7 Participants in the meeting agreed that trust was a key issue for Māori: people want to know who will have their information and how it will be used, and are concerned about the potential for abuse. If Māori are confident that their information will be used in a way that is empowering or mana-enhancing, they will be more willing to agree to the collection and use of that information. If they believe that information will be used in a way that is derogatory to Māori and which diminishes mana, they will be reluctant to share information. Historically, Māori have often been reluctant to provide information to the state. This reluctance can still be seen today in lower rates of participation by Māori in the census, and unwillingness on the part of some Māori to register on the electoral roll.

Iwi and hapū registers

18.8 Privacy principle 2 requires that personal information be collected directly from the individual concerned, unless one of the exceptions applies. It was explained to us that this can create a dilemma for iwi and hapū organisations that want to register people as members. It can be difficult to contact people to ask them to register when they are dispersed throughout the country and many are living

1577 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC R113, Wellington, 2010) 81–82.

overseas. It would be easier if family groups could act on behalf of their members and register them, but this would be inconsistent with principle 2, and it seems unlikely that any of the exceptions would apply. The need to get individual consent to register people can be contrasted with Māori Land Court records of entitlement to rights to Māori land, on which people can be included without express consent. The point was made that iwi and hapū are not like clubs that people have to subscribe to; people are members by virtue of descent. On the other hand, some people may not want to be registered with any tribal authority, or may not want to be registered with a particular authority because they affiliate more strongly to another iwi. It was noted that views will differ among Māori on this issue.

18.9 Some participants in the meeting argued strongly that this was an issue of informed consent. Māori have called on government and the private sector to operate on the basis of prior informed consent in their dealings with Māori, and Māori should operate on the same basis in their dealings with each other. For some participants, this meant that consent should be obtained before people were registered with an iwi or hapū authority. One option that was mentioned would be to register people provisionally when their consent had not been obtained, with the tribal authority then having an obligation to notify such people and seek their consent to being on the register.

18.10 Another issue that was raised with us concerned governance of personal information within tribal authorities. We were told that some iwi authorities keep information about registered members at the centre, without making allowance for hapū that form part of the iwi organisation to use that information for hapū purposes (such as sending out newsletters to hapū members only).[1578] It was suggested that the constitutions of tribal authorities should state clearly the purposes for which personal information about registered tribal members can be used; who has access to the information; and how the information is to be shared between the central authority and its constituent parts.

18.11 The Electoral Act 1993 includes specific provisions in relation to electoral information about iwi affiliation. The Act empowers the Chief Registrar of Electors to seek the consent of electors of Māori descent to the supply of their iwi affiliations and certain other personal information to a designated body.[1579] The Ministers of Justice and Māori Affairs must be satisfied that a body's information management policies and practices comply with the Privacy Act before they can designate that body as being suitable to receive information about iwi affiliations.[1580] Tūhono is the body authorised to receive this information, which it then makes available to iwi organisations representing the iwi to whom Māori electors affiliate.[1581] Just over 100,000 people (around one quarter of registered electors of Māori descent) are registered with Tūhono,

1578 In New Zealand Law Commission *Waka Umanga: A Proposed New Law for Māori Governance Entities* (NZLC R92, Wellington, 2006) 46, the Law Commission commented that: "The modern tendency is for membership registers to be maintained by the central organs of a large tribal entity. This plainly departs from tradition for in the past there was no central organ, only numerous hapū." See also 49–51 of the same Report.

1579 Electoral Act 1993, ss 111B–111F.

1580 Electoral Act 1993, s 111E(3)(c).

1581 www.tuhono.net.

and Tūhono receives regular updates of information about these people from the Electoral Enrolment Centre. The iwi to whom each elector affiliates can access the person's information online, or receive automatic updates, in order to ensure that the information on their databases is up to date.

Māori and online information

18.12 Māori individuals, whānau and organisations are increasingly turning to the internet as a way of keeping in touch and sharing information.[1582] For example, Ngāi Tahu is "moving toward a whānau-controlled social networking space", but is doing so cautiously in order to ensure that privacy and intellectual property are protected.[1583] One issue about the move into the online environment concerns what controls, if any, there should be on the placing of whakapapa information online.[1584] Participants in our June 2008 meeting felt that this is not a matter that should be dealt with by legislation, and that Māori themselves need to address it through education about the need to respect and protect whakapapa information.

Addressing Māori privacy concerns

18.13 We have indicated in chapter 3 that we do not believe that the Privacy Act can easily accommodate the idea of collective or group rights to privacy. To the extent that Māori may see some types of information as belonging to groups rather than individuals, this belief may be better pursued through other areas of the law, such as the developing field of indigenous intellectual property rights. Special mechanisms may also be needed for certain types of sensitive information relating to Māori, even where this information has been anonymised or aggregated so that it does not identify individuals. The creation of the National Kaitiaki Group to oversee the use of information about Māori women from the National Cervical Screening Register is an example of such a mechanism. This would seem to be a matter to be dealt with in specific statutes, rather than within the generic framework of the Privacy Act. There is, however, one mechanism available in the Privacy Act which we believe could be used to recognise privacy interests that go beyond the individual: the ability to bring representative complaints on behalf of a group of individuals who have been affected in similar ways by a privacy breach. We believe there is potential for representative complaints to be brought by whānau, hapū or iwi if an agency were to breach privacy principles in ways that affected the members of Māori collectivities. We ask in chapter 8 whether the Privacy Act should make better provision for representative complaints.

18.14 Our current view is that other privacy issues of particular concern to Māori are probably not matters that can be resolved through amendments to the Act. It was suggested by participants in the meeting we held in June 2008 that the Privacy Commissioner could produce guidance material on the application of the Privacy Act for Māori tribal and other authorities, and could perhaps review provisions about information-handling in the constitutions of Māori authorities. We think there could be a role for the Privacy Commissioner in providing

1582 See Lee Suckling "Cyber Connections" (Makariri/Winter 2009) *Te Karaka* (Ngāi Tahu magazine) 21–23.

1583 Lee Suckling "Cyber Connections" (Makariri/Winter 2009) *Te Karaka* (Ngāi Tahu magazine) 23, quoting Te Rūnanga o Ngāi Tahu Communications Manager Phil Tumataroa.

1584 See discussion in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 106–107.

information and guidance tailored to Māori organisations. We would be interested to receive views on this suggestion, and on whether there are any other ways in which the Privacy Commissioner could better meet the needs of Māori.

18.15 Agencies that handle personal information about Māori can also help to accommodate Māori needs and preferences. Using the flexibility inherent in the Privacy Act, such agencies can modify their handling of Māori personal information in response to Māori concerns.

18.16 While we have no specific proposals for reform in relation to Māori and the Privacy Act, we would welcome suggestions for reforms to either the provisions or the implementation of the Privacy Act to address the issues discussed above, or other issues of particular concern to Māori.

Q185 Are there any ways in which the Privacy Act or the Office of the Privacy Commissioner could better provide for the needs of Māori?

Other cultural groups

18.17 With the exception of Māori, the Law Commission has not looked in any detail at the privacy attitudes and concerns of people from non-European cultural traditions, although we are aware of some research on this issue.[1585] In the Australian state of Victoria, the Office of the Privacy Commissioner commissioned a social research report on privacy issues among indigenous communities and communities from a non-English-speaking background,[1586] and similar research here could be helpful. It would also seem desirable to provide information about people's rights under the Privacy Act in languages other than English.[1587] The Law Commission would welcome other suggestions for action that could be taken to ensure that the Privacy Act meets the needs of people from all cultural and religious backgrounds in New Zealand.

Q186 Are there any ways in which the needs and concerns of particular cultural or religious groups in relation to privacy could be better met?

CHILDREN AND YOUNG PEOPLE

18.18 Children and young people raise special privacy issues. Young children, in particular, are comparatively defenceless and less able to give free consent than adults.[1588] Young people may not have the same understanding of privacy issues or of the consequences of their actions as adults. Consequently, children and young people

1585 See in particular Rowena Cullen "Culture, Identity, and Information Privacy in the Context of Digital Government" (paper presented at the Managing Identity in New Zealand conference, Wellington, 29–30 April 2008); published as "Culture, Identity and Information Privacy in the Age of Digital Government" (2009) 33 Online Information Review 405.

1586 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* (Melbourne, 2002).

1587 In Australia, the Federal and Victorian Offices of the Privacy Commissioner provide information sheets in non-English languages, as does the Broadcasting Standards Authority in New Zealand.

1588 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 203.

can be more vulnerable to invasions of their privacy and may need special protection. At the same time, however, today's young people are sometimes thought to care less about their privacy than previous generations.

18.19 The subject of children and young people's privacy, particularly in the online environment, is one that is increasingly receiving attention internationally. There is growing recognition of young people's vulnerability, and a feeling that special protections may be required.[1589]

18.20 Health information about children and young people raises some complex issues, which we do not deal with here. The Law Commission's approach to health information is discussed in chapter 19.

Young people's attitudes to privacy[1590]

18.21 Attitudes to privacy vary between generations. It has been suggested that today's young people, who have grown up in the world of the internet and mobile phones, may be developing a very different attitude to privacy to that of older generations. Young people's experience of constant connectivity means that their ideas about limiting access to themselves and their information may be different from those of previous generations. Many young people freely make personal information publicly available through blogs and online social networks.

18.22 However, the reality may well be more complex. Studies carried out overseas have found that young people exhibit a range of attitudes to privacy. The majority do exercise some caution in relation to disclosing their personal information online. The privacy issues that concern young people may well be different from the issues that concern older generations: for example, the Australian Law Reform Commission (ALRC) found that young people tended to be less concerned about government accessing their personal information than older generations.[1591] Nonetheless, young people place high importance on being able to exercise control over their own information. Furthermore, some young people's apparent willingness to disclose personal information may stem from a lack of understanding of the potential privacy risks involved, or from young people's tendency to take risks, or from a desire to fit in with their peer group,[1592] rather than necessarily reflecting a lack of concern for their privacy.

1589 See, eg, Resolution on Children's Online Privacy (30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 15–17 October 2008); Article 29 Data Protection Working Party "Opinion 2/2009 on the protection of children's personal data" (11 February 2009) 398/09/EN WP160.

1590 We have explored this topic more fully in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 108–113. See also Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) ch 67; John Palfrey and Urs Gasser *Born Digital: Understanding the First Generation of Digital Natives* (Basic Books, New York, 2008) chs 1–4.

1591 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 67.46.

1592 See, for example, Danielle Wong "Popularity Outweighs Facebook Privacy Fears" (25 August 2009) *The Star* Canada www.thestar.com (accessed 20 January 2010).

Young people and the Privacy Act

18.23 The Privacy Act does not generally make specific provision for information relating to young people at present. The Act applies in the same way to everyone, regardless of age. The only specific mention of age is in section 29(1)(d), which provides that an agency may refuse to disclose personal information requested under principle 6 if, in the case of an individual under the age of 16, the disclosure of that information would be contrary to that individual's interests.

18.24 The Health Act 1956 and the Health Information Privacy Code 1994 (HIPC), which modifies the privacy principles for the health sector, also make some provision for young people. Section 22F(1) of the Health Act provides that:

> Every person who holds health information of any kind shall, at the request of the individual about whom the information is held, or a representative of that individual, or any other person that is providing, or is to provide, services to that individual, disclose that information to that individual or, as the case requires, to that representative or to that other person.

Rule 11(4) of the Code provides:

> Where, under section 22F(1) of the Health Act 1956, the individual concerned or a representative of that individual requests the disclosure of health information to that individual or representative, a health agency—
>
> (a) must treat any request by that individual as if it were a health information privacy request made under rule 6; and
>
> (b) may refuse to disclose information to the representative if—
>
> (i) the disclosure of the information would be contrary to the individual's interests; or
>
> (ii) the agency has reasonable grounds for believing that the individual does not or would not wish the information to be disclosed; or
>
> (iii) there would be good grounds for withholding the information under Part 4 of the Act if the request had been made by the individual concerned.

The Code defines a representative as:

> (a) where that individual is dead, that individual's personal representative; or
>
> (b) where the individual is under the age of 16 years, that individual's parent or guardian; or
>
> (c) where the individual, not being an individual referred to in paragraphs (a) or (b), is unable to give his or her consent or authority, or exercise his or her rights, a person appearing to be lawfully acting on the individual's behalf or in his or her interests.

In other words, parents or guardians of children under 16 may access their children's health information, but health agencies may also legitimately withhold such information from parents or guardians in some cases.

18.25 There have sometimes been perceptions that the Privacy Act prevents parents from finding out information about their children. For example, there have been stories of the Act being used to withhold children's school reports from their parents, but in most cases there are no grounds for withholding such reports

under the Privacy Act or other legislation.[1593] While such perceptions are usually exaggerated or untrue, the Act does treat children and young people as individuals capable of exercising rights. As such, parents are not automatically entitled to access their children's personal information in all situations. We consider in the next section whether the Act should make provision for the age at which young people are presumed to have the capacity to give consent and exercise rights under the Act.

Issues for reform

Should the Act contain additional protections for young people?

18.26 Given the issues we have noted regarding the vulnerability of children and young people, it is worth asking whether the Act should contain additional safeguards for them. The South African Law Reform Commission has suggested that "children should … first of all be protected against their own immaturity and, secondly, against malicious third parties."[1594]

18.27 We outline below some areas where additional protections might be considered, but welcome any submissions.

18.28 Non-legal actions could also be valuable in this area. Educating children and young people about privacy risks and how to avoid or mitigate them would go a long way to address some of the privacy concerns about children and young people. The Privacy Commissioner's education functions can usefully be exercised to this end, and indeed the Commissioner is already doing so. OPC has recently established a focus group of young people to assist with its work in this area. The organisation Netsafe is also carrying out valuable educational work about online privacy and safety issues for children and young people in New Zealand.[1595] The ALRC has recommended that the Office of the Federal Privacy Commissioner should develop and publish educational material about privacy issues aimed at children and young people, and also that education about privacy, particularly online, should be incorporated into school curricula.[1596]

Online privacy

18.29 Privacy in the online environment is one area that has been identified where children and young people may need special protections. Particular risks for young people online include invasion of privacy, cyber bullying and sexual exploitation.[1597] Young people's seeming willingness to disclose information

1593 See Kathryn Dalziel *Privacy in Schools: A Guide to the Privacy Act for Principals, Teachers and Boards of Trustees* (Office of the Privacy Commissioner, Wellington, 2009) 30.

1594 South African Law Reform Commission *Privacy and Data Protection: Report* (SALRC Project 124, Pretoria, 2009) para 4.3.18.

1595 www.netsafe.org.nz.

1596 Australian Law Reform Commission *For Your Information: Australian Privacy Law And Practice* (ALRC R108, Sydney, 2008) recommendations 67-2, 67-3 and 67-4.

1597 Working Group of Canadian Privacy Commissioners and Child and Youth Advocates *There Ought to be a Law: Protecting Children's Online Privacy in the 21st Century* (2009) 8–12.

about themselves over the internet may mean that they put themselves at risks (for example, of identity crime) or disclose information that they later may wish to be private.

18.30 Commercialisation of children's online space has also been raised as a concern. Many sites targeted at children collect personal information from children, for example through participation in online quizzes and games which record the user's likes and dislikes. This information is then used for marketing purposes. It may not be apparent to children that their information will be used in this way. Furthermore, many of these sites blend commercial content and entertainment. Children typically cannot differentiate between online content and advertising as well as adults can, so are more susceptible to marketing through these sites.

18.31 There have been overseas law reform initiatives to address this issue. The most notable is the United States Children's Online Privacy Protection Act of 1998.[1598] The law applies to operators of commercial websites directed at children that collect personal information from children under the age of 13. Website operators must obtain "verifiable" parental consent before collecting personal information from children under 13. In practice, this has meant that the operator must make reasonable efforts to provide parents with notice of its information collecting practices and ensure that they give consent on this basis. The Act has been criticised as being ineffective for a number of reasons, including difficulties in verifying parental consent, and the fact that many website privacy policies are difficult to understand and are not read by users.[1599]

Direct marketing to children and young people

18.32 A related issue is direct marketing to young people. We discuss direct marketing in chapter 13. However, there are some concerns specific to young people.[1600] Children may be more susceptible to commercial influence, and less able to recognise some forms of advertising, than adults. Furthermore, the internet has enabled direct marketers to target children in an environment where they are often unsupervised. There have been suggestions that direct marketing to children and young people should be limited or banned outright. The Advertising Standards Authority has a Code for Advertising to Children, which draws attention to principle 3 of the Privacy Act and states that:[1601]

> Extreme care should be taken in requesting or recording the names, addresses and other personal details of children to ensure that children's privacy rights are fully protected and the information is not used in an inappropriate manner.

1598 91 USC § 6501–6506.

1599 Working Group of Canadian Privacy Commissioners and Child and Youth Advocates *There Ought to be a Law: Protecting Children's Online Privacy in the 21st Century* (2009) 13.

1600 Anna Fielder, Will Gardner, Agnes Nairn and Jillian Pitt *Fair Game? Assessing Commercial Activity on Children's Favourite Websites and Online Environments* (National Consumer Council, London, 2007); Working Group of Canadian Privacy Commissioners and Child and Youth Advocates *There Ought to be a Law: Protecting Children's Online Privacy in the 21st Century* (2009) 7–9.

1601 Advertising Standards Authority *Code of Advertising to Children* (2006) Guideline 4(c) www.asa.co.nz/code_children.php.

18.33 The Law Commission does not at this stage propose any reforms in this area, but is interested in submitters' views on this subject.

Q187 Are any particular protections for young people required in relation to online privacy or direct marketing?

Q188 Are any other new, specific protections for young people needed in the Act?

Age of presumption of capacity

18.34 Issues may arise with children and young people because they are still developing physically and mentally. In practice, children often need to exercise their rights under the Act through a representative, usually a parent or guardian. However, the child's best interest can sometimes confer upon the child privacy rights which may override the wishes of parents or other representatives. As children mature they can be expected to become more involved in decisions relating to their personal information, and are increasingly able to exercise their own rights.[1602]

18.35 Currently, decisions about whether a young person has sufficient understanding and maturity to be capable of exercising rights under the Act seem to be dealt with on a case-by-case basis. Exceptions to the privacy principles will often apply to allow parents to act on behalf of a child: for example, information may be collected from parents rather than directly from the child under one of the exceptions to principle 2.

18.36 There is a question about whether the Act should make specific provision regarding the age at which one can exercise rights, such as the right to consent to collection of personal information or to make an access request.

18.37 Such a provision would perhaps provide more clarity for agencies dealing with young people, such as schools and hospitals. However, there are some potential problems, such as verifying age. Often personal information is collected over the phone or internet, so it would be difficult for agencies to assess whether the person they are dealing with is of the required age. A specified age at which rights under the Act can be exercised also seems rather inflexible compared to the current position. It could deprive young people of the opportunity to take responsibility for their own personal information in situations where they are capable of doing so but are under the requisite age.

18.38 Another option would be to provide that an assessment of the child or young person's maturity should be carried out in order to determine whether they have capacity to exercise their own rights. This seems to be the position in fact now, but there may be thought to be advantages in specifying it clearly, even though implementation of it might often raise considerable practical difficulties.

1602 See Article 29 Data Protection Working Party "Opinion 2/2009 on the Protection of Children's Personal Data" (11 February 2009) 398/09/EN WP160 paras 4–7.

18.39 Internationally, most privacy legislation takes a similar approach to New Zealand's, treating all individuals the same, regardless of age. This is in line with obligations under the United Nations Convention on the Rights of the Child to respect children's right to privacy.[1603]

18.40 The ALRC has recommended that the Australian Privacy Act be amended to provide that where it is reasonable and practicable to make an assessment about the capacity of an individual under the age of 18 to give consent, make a request or exercise a right of access under the Act, an assessment about the individual's capacity should be undertaken. Where an assessment of capacity is not reasonable or practicable, then an individual:

(a) aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access; and

(b) under the age of 15 is presumed to be incapable of giving consent, making a request or exercising a right of access.[1604]

At the time of writing, the Australian government had not yet responded to this recommendation.

Q189 Should the Act provide more specifically for when a child or young person should be treated as having capacity to exercise rights under the Act? If so, should there be a set age or a more individual test?

Q190 Do you have any other concerns about the privacy of children and young people?

ADULTS WITH REDUCED CAPACITY

18.41 For various reasons, some adults have a reduced capacity to act on their own behalf, and particularly to exercise the power to give or withhold consent to the collection, use or disclosure of their personal information. This includes individuals with various forms of intellectual disability and mental illness. The Privacy Act makes no specific provision for such people.

18.42 There is a presumption in common law that all adults have capacity until the contrary is proved. This presumption is also included in section 5 of the Protection of Personal and Property Rights Act 1988. Except as provided for under that Act, all persons subject to an order made under the Act are presumed to have the same legal capacity as any other person.[1605] The Protection of Personal and Property Rights Act also provides that, in relation to applications made under the Act, courts are to make the least-restrictive intervention possible in the lives of those in respect of whom applications are made, and are to encourage those persons to exercise such capacity as they have to the greatest extent possible.[1606]

1603 Convention on the Rights of the Child (20 November 1989) 1577 UNTS 3, art 16.

1604 Australian Law Reform Commission *For Your Information: Australian Privacy Law And Practice* (ALRC R108, Sydney, 2008) recommendation 68-1.

1605 Protection of Personal and Property Rights Act 1988, s 4.

1606 Protection of Personal and Property Rights Act 1988, s 8.

18.43 New Zealand law provides various forms of recognition of the need in some circumstances for another person to make decisions on behalf of a person with a temporary or permanent incapacity. These include welfare guardianship, enduring powers of attorney, and advance directives.

18.44 The key questions for consideration are:

- Does the Privacy Act need to make express provision for people who are acting under legal authority for other individuals who are affected by some form of incapacity?
- Does the Privacy Act need to make any provision for adults with reduced capacity, where such adults do not have a legally-recognised representative?

18.45 The ALRC considered issues relating to adults with a temporary or permanent incapacity, and came to the following conclusions in its final report:[1607]

- A test for assessment of capacity should not be set out in the Privacy Act 1988 (Cth), but should be dealt with by guidance from the Office of the Privacy Commissioner.
- Substitute decision-makers are already empowered by relevant laws to act on behalf of an individual, and it is not necessary for the Privacy Act to provide for substitute decision-makers authorised by law.
- The Privacy Act should not recognise informal representatives (such as family members) who are not substitute decision-makers authorised by law and who are not acting with the consent of the individual concerned. Such recognition would constitute an unacceptable risk to privacy.

18.46 It is important to note that the New Zealand Privacy Act does not have a positive requirement of consent to the collection, use or disclosure of personal information. Rather, consent is one of a number of exceptions to the privacy principles. Thus, it is not necessarily the case that the consent of a person with reduced capacity is required in order to collect, use or disclose that person's information – it may be possible to rely on one of the other exceptions. Nonetheless, there will be situations in which none of the other exceptions apply, and the question of consent is central to the handling of an individual's information. The 1996 Mason Inquiry into mental health services referred to what it called the "patient veto" on disclosure of personal information where "a patient is clearly unwell and has lost the insight to act in his or her best interests". The inquiry's report suggested that:[1608]

> There may need to be a specially designated person or office holder who could adjudicate or decide [in circumstances where a mentally unwell patient gives express instructions not to disclose information] as to whether or not there should be disclosure and if so to what extent. Another possibility may be a provision that disclosure of particular information to a particular class of persons would not constitute an interference with privacy under the Privacy Act 1993.

1607 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 2344–2361.

1608 Ken Mason, June Johnston and Jim Crowe *Inquiry under Section 47 of the Health and Disability Services Act 1993 in Respect of Certain Mental Health Services: Report of the Ministerial Inquiry to the Minister of Health Hon Jenny Shipley* (1996) 53.

18.47 As we have already noted in relation to children and young people, the HIPC includes provisions relating to disclosure of health information to a person's representative. "Representative" as defined in the Code includes "a person appearing to be lawfully acting" on behalf of, or in the interests of, an individual who is unable to give his or her consent or authority, or to exercise his or her rights. Rule 11(1) of the HIPC allows for the disclosure of an individual's health information when such disclosure is to, or is authorised by, the individual's representative, and where the individual is unable to exercise his or her rights or to give his or her authority.[1609] Section 22F(1) of the Health Act 1956 and HIPC rule 11(4), quoted in the section on children and young people above, also allow for disclosure of health information to a person's representative, although at the same time they provide for such information to be withheld on certain grounds.

18.48 In addition, HIPC rule 11(2)(b) allows the disclosure of an individual's health information to a person nominated by the individual, to the individual's principal caregiver, or to a near relative of the individual if it is not desirable or not practical to obtain the individual's authorisation and the disclosure is not contrary to the expressed request of the individual or his or her representative. The Privacy Commissioner's Commentary on this sub-rule states that:[1610]

> Difficulties may arise with patients who move in and out of psychiatric institutions and the care of a family member or caregiver. Often at the time of re-admission such patients may be hostile to their caregivers and veto the giving of any information to them. There is no easy solution to this issue but the rule does require respect for clear instructions by the patient.

18.49 In recognition of the fact that mental health information raises some particularly complex issues, OPC and the Mental Health Commissioner have developed guidance material for health practitioners in relation to such information.[1611] This guidance includes discussion of dealing with representatives and families.

Q191 Should the Privacy Act include any special provisions for adults with reduced capacity?

OTHER GROUPS

18.50 There may be other groups within the wider society that have particular privacy needs and concerns: for example, people with disabilities. The Law Commission would welcome submissions identifying such needs and concerns, and suggesting ways of addressing them.

Q192 Are there any other groups that have particular needs in relation to the Privacy Act? If so, how should these be provided for?

1609 Health Information Privacy Code 1994, r 11(1)(a)(ii) and (b)(ii).

1610 Privacy Commissioner *Health Information Privacy Code 1994 Incorporating Amendments and Including Revised Commentary* (Office of the Privacy Commissioner, Wellington, 2008) 63.

1611 The Privacy Commissioner has recently sought public comment on a revised version of this guidance: Mental Health Commission and Office of the Privacy Commissioner *Guidance Material for Health Practitioners on Mental Health Information* (2009).

Chapter 19

Health information and workplace privacy

19.1 In this chapter we discuss two important areas of privacy: health information and workplace privacy. These are both large and complex subjects in their own right. We thus have not been able to cover them in depth in this review. However we feel it is important to highlight these topics and suggest that further work may well need to be done on them. This chapter provides a brief outline of the potential issues in each area and asks for submitters' views.

HEALTH INFORMATION[1612] Context and issues

19.2 Information is vital to health care. In the course of medical treatment, a wide variety of personal information might be required and/or used: for example information about the patient's medical history and lifestyle, family history, diagnosis, treatment, current medications, vital signs (temperature, respiratory rate, blood pressure, blood oxygen, heart rate and level of consciousness). Furthermore, in determining the appropriate treatment clinicians draw on population data and medical research. Health information systems are therefore critical, and their effectiveness affects the quality of care.[1613]

19.3 Sharing personal information between health practitioners can also be critical to patient care. Healthcare requires interactions between different practitioners such as general practitioners, specialists, pathologists, pharmacists and nurses. People from other sectors, such as social workers, may also be involved. All these individuals need to be able to work together and to communicate about patients. Patients' medical records must be available to those treating them at each stage in the medical system. In emergencies, it is vital that such information be available quickly. As such, there is an increasing drive to share health information for benefit of patients and the wider community. The future health of citizens also depends on medical research. Researchers need access to case information.

1612 We have previously discussed this subject in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 204–209.

1613 Rowena Cullen "Why IT matters: your health and the public health" (Inaugural Professorial Lecture, Victoria University of Wellington, 13 October 2009).

19.4 While disclosure of health information to appropriate persons is important, privacy and confidentiality are also especially important in health. Maintaining confidentiality is essential to the doctor/patient relationship, to ensure patient trust. Without an assurance that their personal health information will be protected, people might not seek help when they need it. This also encourages public trust in the health system as a whole. There is therefore an individual and public interest in ensuring the privacy of personal health information. Health information is also sensitive information due to its personal nature. There is a difficult balance to be struck between keeping personal information confidential on the one hand, and getting the right information to the right person at the right time on the other. It is important that patients are aware of how their information will be used.

19.5 Technological developments have enabled new ways of collecting and storing health information. Computerised data collection, storage and dissemination can raise privacy concerns, as information can be networked and shared more easily. The possibility of having a single electronic health record for each individual is one that is gaining popularity internationally, but also has potential privacy implications as the information would be more vulnerable.[1614] Developments in genetic testing also raise difficult privacy issues.

Current law

19.6 The law governing health information and privacy is principally made up of the Privacy Act and Health Information Privacy Code, together with the Health Act 1956. There are further provisions scattered across a number of other statutes.[1615]

19.7 The most important aspect of the Privacy Act is the exception to principle 11 where the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to public health or public safety, or to the life or health of the individual concerned or another individual.[1616] We have discussed possible modifications to this exception in chapter 4.

Health Information Privacy Code 1994

19.8 The Health Information Privacy Code 1994 (the Code) modifies the information privacy principles in relation to health information about identifiable individuals. It governs the collection, holding, use and disclosure by health agencies of personal information relating to health. It 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.

1614 See, for example, Marie Shroff, Privacy Commissioner "Talking Privacy" (12 August 2009) *New Zealand Doctor.*

1615 See, for example, Human Assisted Reproduction Act 2004, s 66; Public Health and Disability Act 2000, s 18(7). For a full description of the legal framework governing health information see PDG Skegg and Ron Paterson (eds) *Medical Law in New Zealand* (Brookers, Wellington, 2006) chapters 9–12.

1616 Privacy Act 1993, s 6, principle 11(f).

Health Act 1956

19.9 The Health Act 1956 also has provisions relating to personal health information. It overrides the Code to the extent that there is any inconsistency between them. Sections 22B to 22H deal with personal information.[1617]

19.10 Section 22C governs disclosure of health information. It provides that health information may be disclosed if required by certain persons, who are generally state employees such as social workers, prison officers or district health board (DHB) employees. Health information may also be disclosed if permitted by the Code. Disclosure may be authorised by an individual who is over 16 or their representative.

19.11 Section 22D provides that the Minister may require DHBs to provide information for the purposes of obtaining statistics. Under section 22E, the Minister may also require DHBs to provide information for the purposes of blood collection.

19.12 Section 22F provides that anyone who holds health information about an individual must disclose the information if requested by the individual concerned, their representative or any person providing services to them. There are exceptions where there is a lawful excuse to refuse, there are reasonable grounds to believe that the individual concerned does not want the information to be disclosed, or refusal is authorised by the Code.

19.13 Section 22G relates to inspection of records for the purpose of verifying a claim for payment.

19.14 Section 22H provides that, regardless of any other law, health information may be disclosed if it does not permit identification of the person whom it is about.

Reform

19.15 This is a complex and sensitive area. The current legal framework is not very coherent. Furthermore, there are concerns in some quarters that the current law, or more likely misunderstandings of what is allowed, can cause the withholding of critical information with, at times, very unfortunate results. Coroners have recently made comment to this effect. We have also heard that medical researchers are sometimes concerned about the availability of information that they need. In light of this, we feel that health information and privacy are in need of separate, expert, study.

19.16 Given the complexities of this area and the importance of healthcare in New Zealand, the Law Commission feels that it is worth considering enacting separate legislation governing health information, setting out a clear framework for:

- 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.

1617 The Public Health Bill 2007, no 177-2 is currently before the House and would replace the Health Act 1956. Clauses 20–26 of the Bill largely replicate sections 22B–22H.

There are overseas examples of specific legislation governing health information privacy.[1618] What we have in mind, however, goes beyond privacy and would cover how health information as a whole is handled.

19.17 The Ministry of Health is currently working on a project on health information and how it is used. We think that any further work on this topic should await the outcome of the Ministry's work.

Q193 Is there a need for a separate review of health information and/or new health information legislation?

WORKPLACE PRIVACY[1619]

19.18 Workplace privacy raises a number of issues, many of which do not directly relate to the Privacy Act. We discuss issues to do with surveillance in the workplace in stage 3 of our Review. This section deals with workplace privacy as it relates to the Act.

Context and issues

19.19 People spend a significant amount of their time at work, and employers hold large amounts of personal information about their employees. This generally includes employees' bank account details, IRD number, salary information, CVs, performance reviews and medical information. Some of this information is very sensitive.

19.20 Furthermore, employers often want or need to limit the privacy of employees in order to increase productivity, protect their property or avoid liability. To this end, they may engage in activities such as surveillance and monitoring of workers (for example, monitoring hours worked, internet or email use), and physical and psychological testing (for example, drug or alcohol testing).[1620] Again, new technologies are increasing the potential for employers to gather more information about employees.[1621] Current issues include DNA testing of employees and the use of biometrics to monitor employees (for example, the use of finger scanning for employees to "clock in" and "clock out").

19.21 Privacy in the workplace may arguably require more or different protection, due to the particular nature of the employment relationship. There is an imbalance of power in the employer/employee relationship, which can cause privacy challenges in terms of issues such as consent. Employees may often be asked to consent to certain practices as part of their employment contract, but it is difficult for employees to give true consent to privacy invasive practices in the workplace. Refusing would often effectively mean turning down an offer of employment, which many people may not be in a position to do.

1618 See, for example, E-Health (Personal Health Information Access and Protection of Privacy) Bill (British Columbia); Health Records and Information Privacy Act 2002 (NSW); Health Records Act 2001 (Vic); Health Records (Privacy and Access) Act 1997 (ACT).

1619 We have previously discussed this subject in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 214–218.

1620 Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65, 66–71.

1621 See, for example, Privacy International *PHR2006 – Privacy Topics – Workplace Privacy* www.privacyinternational.org (accessed 31 October 2008).

Current law

19.22 The law on workplace privacy is currently scattered across a number of statutes. The Employment Relations Act 2000 provides the framework for the employer-employee relationship and imposes mutual obligations of trust and confidence and good faith. 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, for example not to endanger themselves or others. These duties may sometimes justify a lesser degree of privacy in order to ensure safety (for example, monitoring). Discriminatory treatment by employers is covered by both the Employment Relations Act 2000 and Human Rights Act 1993. The Privacy Act applies to personal information held by employers about employees, and the tort of invasion of privacy may also apply in some cases.

19.23 The question is whether the existing legal framework achieves the correct balance between the privacy interests of employees and employers' interests such as productivity and ensuring a safe work environment. Some have argued that the current law favours employers' interests over employees' privacy.[1622] We are interested in submissions on whether the current legal framework is working effectively and whether workplace privacy should be the subject of specific rules, rather than being governed by the general law as now.

Potential reform

19.24 Potential options for reform of the law on workplace privacy include:

- the status quo;
- specific workplace privacy legislation;
- a code of practice under the Privacy Act, specifying how the privacy principles apply in the workplace;
- a code of employment practice under section 100A of the Employment Relations Act, providing guidance on how the Act applies to privacy;
- codes developed by industries; or
- guidance given by the Privacy Commissioner (we note that the Commissioner has already published a guide to the Privacy Act for employers and employees[1623]).

19.25 Internationally, there have been a number of reforms related to workplace privacy. Finland has introduced comprehensive legislation regulating drug testing, personality and aptitude tests, genetic testing, surveillance and email monitoring. Privacy Commissioners in the UK, Hong Kong and Ontario have issued codes and guidelines on workplace privacy issues.[1624]

1622 Paul Roth "Privacy in the Workplace – Getting the Balance Right?" (Paper presented to Privacy Issues Forum, Christchurch, 13 June 1996), cited in Rebecca Britton "An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand" (2006) 12 Canta LR 65, 89.

1623 Office of the Privacy Commissioner *Privacy at work* (Wellington, 2008).

1624 Examples taken from Victorian Law Reform Commission *Workplace Privacy: Final Report* (Victorian Government Printer, Melbourne, 2005) 24–25.

19.26 Workplace privacy reform has also been considered in a number of Australian states.[1625] The most comprehensive is the Victorian Law Reform Commission's proposal for a Workplace Privacy Bill.[1626] The Bill, which has not been enacted, would impose an obligation on employers not to unreasonably breach the privacy of prospective workers or workers while they are working. Unreasonable breaches are described as acts or practices carried out for a purpose not directly connected to the employer's business, in a manner that is not proportionate to the act or practice's purpose, without first taking reasonable steps to inform and consult with workers or without providing adequate privacy safeguards. Furthermore, acts or practices that affect workers' privacy when they are not working, or where they are subject to genetic testing, would require authorisation, and surveillance in private areas of the workplace would be prohibited entirely. The regulator would have the power to issue advisory and mandatory codes of practice.

19.27 In our consultations for stage 3 of this Review, we found no enthusiasm for codifying the law on workplace privacy. However, as we have said, the focus in those consultations was on surveillance and intrusion in the workplace.[1627] This issues paper is concerned with the Privacy Act, so the question we ask here is concerned with the Act and its interaction with other laws governing workplace privacy.

Q194 Are you satisfied with the current legal framework governing workplace privacy, or is more specific regulation, such as a code of practice or specific legislation, needed to deal with workplace privacy issues?

OTHER ISSUES

Q195 Do you have any other comments, or any further suggestions, about how the Privacy Act 1993 could be amended or improved?

1625 Note that employee records are not covered by Australian Federal privacy legislation: Privacy Act 1988 (Cth), s 6.

1626 Victorian Law Reform Commission *Workplace Privacy: Final Report* (Victorian Government Printer, Melbourne, 2005).

1627 See New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2009) 291–296 for discussion and questions on which we sought submissions, and New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, Wellington, 2010) 86–87 for our conclusions on workplace surveillance.

Appendices

Appendix A
The privacy principles

Principle 1: Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

(a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) the collection of the information is necessary for that purpose.

Principle 2: Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—

(a) that the information is publicly available information; or

(b) that the individual concerned authorises collection of the information from someone else; or

(c) that non-compliance would not prejudice the interests of the individual concerned; or

(d) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(e) that compliance would prejudice the purposes of the collection; or

(f) that compliance is not reasonably practicable in the circumstances of the particular case; or

(g) that the information—

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) That the collection of the information is in accordance with an authority granted under section 54.

Principle 3: Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) the fact that the information is being collected; and

(b) the purpose for which the information is being collected; and

(c) the intended recipients of the information; and

(d) the name and address of—

(i) the agency that is collecting the information; and

(ii) the agency that will hold the information; and

(e) if the collection of the information is authorised or required by or under law,—

(i) the particular law by or under which the collection of the information is so authorised or required; and

(ii) whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) the rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—

(a) that non-compliance is authorised by the individual concerned; or

(b) that non-compliance would not prejudice the interests of the individual concerned; or

(c) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that compliance would prejudice the purposes of the collection; or

(e) that compliance is not reasonably practicable in the circumstances of the particular case; or

(f) that the information—

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4: Manner of collection of personal information

Personal information shall not be collected by an agency—

(a) by unlawful means; or

(b) by means that, in the circumstances of the case,—

(i) are unfair; or

(ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5: Storage and security of personal information

An agency that holds personal information shall ensure—

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6: Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) to have access to that information.

(2) Where, in accordance with subclause (1)(b), an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5.

Principle 7: Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—

(a) to request correction of the information; and

(b) to request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3), the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1), the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8: Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9: Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10: Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—

(a) that the source of the information is a publicly available publication; or

(b) that the use of the information for that other purpose is authorised by the individual concerned; or

(c) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) that the information—

(i) is used in a form in which the individual concerned is not identified; or

(ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) that the use of the information is in accordance with an authority granted under section 54.

Principle 11: Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under section 54.

Principle 12: Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007 (to the extent to which those rules apply for the whole of that Act excluding the 1973, 1988, and 1990 version provisions).

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

Appendix B
List of questions

The Commission welcomes your views on the following questions. Feel free to answer as many or as few questions as you like.

CHAPTER 2 SCOPE, APPROACH AND STRUCTURE OF THE ACT

Q1 We believe that the "principles-based", open-textured approach to information privacy regulation in New Zealand is still appropriate. Do you agree? What problems have been encountered as a result of this approach? In what circumstances has it been shown to be helpful or appropriate? What other approaches or combinations of approaches might be more appropriate?

Q2 Do you think the Privacy Act strikes the right balance between privacy and other competing interests?

Q3 Are there ways in which compliance with the Act can be made easier and less costly without compromising its objectives?

Q4 Should the name of the Privacy Act be changed? If so, what should its new name be? Should the Privacy Commissioner be called something else, such as the Data Protection Commissioner?

Q5 Should the Privacy Act contain a purpose clause? If so, what should it say?

Q6 How might the Privacy Act be better structured so that it is easier to navigate and to read?

Q7 How is the Act perceived to be operating in practice? Are any perceived deficiencies the result of the Act itself, or rather of the way it is understood and applied? Could any changes to the Act be made so that the public perception and understanding of it more correctly match its objectives?

Q8 Do you find the guidance issued by the Privacy Commissioner useful? On what topics would you like more such guidance?

CHAPTER 3 KEY DEFINITIONS

Q9 Do the following elements of the definition of "personal information" in the Privacy Act need to be clarified? If so, do you have any suggestions about how this should be done?

- "information"
- "about"
- "identifiable"

Q10 Are there any other issues you would like to raise about the definition of "personal information"?

Q11 Do you agree that human tissue samples should not be covered by the definition of personal information in the Privacy Act? Why, or why not?

Q12 Is any clarification needed with regard to the coverage by the privacy principles of genetic information or other information derived from bodily samples?

Q13 Should there be any changes to the existing provisions relating to deceased persons in the Privacy Act? (See in particular the proposals in paragraphs 3.52 and 3.55.)

Q14 We propose that the Privacy Act should be amended to allow codes of practice to apply any of the privacy principles to information about deceased persons. Do you agree?

Q15 Should any other amendments be made to the Privacy Act to extend its application to information about deceased persons?

Q16 We propose that the Privacy Act should be amended to make clear that section 3(1) of the Law Reform Act 1936 applies to causes of action under the Privacy Act. Do you agree? Do you have any other suggestions about survival of Privacy Act complaints after death?

Q17 Should the Act provide that any code of practice relating to the credit reporting industry may provide for access and correction rights for corporations? Should the Act provide generally for access and correction rights for corporations?

Q18 We propose that the Privacy Act should be amended to make clear that, despite the general exclusion of information about legal persons from the definition of personal information, information about a legal person can be personal information if it is also clearly information about an identifiable individual. Do you agree? Would this have implications for other areas of law?

Q19 Should the Privacy Act be amended to clarify the circumstances in which information about a trust can be personal information?

Q20 We propose that the definition of "collect" should be deleted. Do you agree? If not, should it be clarified in some way?

Q21 Are there any other terms that need to be defined, or whose definitions should be amended?

Q22 Should any of the existing principles be combined?

Q23 Should principle 12 be removed from the principles and placed somewhere else in the Act?

Q24 Should any other principles be deleted?

Q25 Should there be any structural changes to the exceptions to the principles?

Q26 Are you aware of situations in which the purposes for which agencies collect information are unclear? Does a lack of clarity about the purpose for which agencies collect information sometimes cause problems? Do you have any suggestions about how the Act should deal with specification of purpose?

Q27 Should principle 1 be amended to require that the collection of information is *reasonably* necessary for the purpose? If so, how should reasonableness be determined?

Q28 We propose that the word "directly" should be deleted from principles 2(1) and 3(1). Do you agree?

Q29 We propose that principle 2 should provide that unsolicited information must either be destroyed; or, if it is retained, handled in compliance with all relevant provisions of the privacy principles as if the agency had take active steps to collect it. Do you agree? We further propose that principle 2 should provide that an agency must not retain unsolicited information that it would be unlawful for it to collect. Do you agree? Do you have any other suggestions with regard to the handling of unsolicited information?

Q30 Should principle 3 be amended by making it applicable whether or not the information is collected from the person concerned?

Q31 We propose that the "no prejudice" exception to principles 2 and 3 should be deleted. Do you agree?

Q32 Should the Act provide that the "not reasonably practicable" exception does not apply when an agency wishes to avoid complying with principle 2 simply because the individual concerned refuses to provide the information, or because the agency believes that the individual would refuse?

Q33 We propose that a "health or safety" exception should be added to principle 2. Do you agree? Should such an exception also be added to principle 3?

Q34 We propose that the exceptions in principle 3(4)(a) and 3(4)(f)(ii) should be deleted. Do you agree?

Q35 We propose that principle 4 should be amended so that it clearly applies to *attempts* to collect information. Do you agree?

Q36 We propose that principle 5 should be amended to make clear that agencies must take reasonable steps to ensure that people who are authorised to access personal information for the purposes in connection with which the information is held by the agency do not access, use, modify or disclose that information for other purposes. Do you agree?

Q37 We propose that principle 8 should be amended so that agencies must check the accuracy of information before use *or disclosure*. Do you agree?

Q38 We propose that principle 9 should continue to allow retention of information for so long as it is required for the purposes for which it may lawfully be used. Do you agree?

Q39 We propose that principle 9 should continue not to specify how personal information should be disposed of. Do you agree? Would guidance on this point from the Office of the Privacy Commissioner be helpful?

Q40 Are coerced access requests a problem? If so, can the Privacy Act be amended to deal with the problem?

Q41 We propose that where an agency is not willing to correct personal information, it should be required to inform the requester of his or her right to request that a statement be attached to the information of the correction sought but not made. Do you agree?

Q42 Should the "safety" ground in section 27(1)(d) be expanded? If so, what new elements should it contain?

Q43 Should there be a specific withholding ground relating to significant likelihood of harassment, or do existing withholding grounds cover this adequately?

Q44 Should the "commercial prejudice" withholding ground in section 28(1)(b) be amended? If so, how?

Q45 Should the Privacy Act be amended to provide statutory guidance with respect to the withholding of information under section 29(1)(a) in cases of "mixed" information? If not, would guidance from the Privacy Commissioner be of assistance?

Q46 Should section 29(1)(c) be amended to refer to consulting the individual's psychologist when appropriate? Should it refer to consulting with any other health practitioners and, if so, which ones?

Q47 We propose that a new ground for refusal should be added to allow agencies to refuse access to information that has previously been provided to an individual, or that has previously been refused, provided that no reasonable grounds exist for the individual to request the information again. Do you agree? Do you have any other suggestions about how the Privacy Act should deal with the problem of repeated access requests for the same information?

Q48 We propose that private sector agencies should no longer be allowed to charge for correction of personal information. Do you agree?

Q49 We propose that complexity of the issues raised by a personal information request should be added to the grounds for seeking an extension of time in section 41(1). Do you agree?

Q50 Should the Act expressly provide that disclosures within agencies can be covered by principle 11? If so, how should this be done?

Q51 Should there be a new exception to principle 11 where the disclosure is to a person or persons who already know the information in question?

Q52 We propose that the words "and imminent" should be deleted from principles 10(d) and 11(f). Do you agree?

Q53 Should "assign" or "identifier" be defined in the Act, and if so, how should they be defined?

Q54 Should principle 12(2) be amended so that it applies only to unique identifiers originally generated, created or assigned by public sector agencies (with an accompanying amendment to section 46(4) to allow principle 12(2) to be reapplied to private sector-generated identifiers by a code of practice)?

Q55 Should there be an exception to principle 12(2) for statistical and research purposes? Should there be any other exceptions to principle 12(2)?

Q56 Is there any uncertainty about the application of principle 12(4)? If so, how should this be addressed?

Q57 Are any other changes needed to any of the existing privacy principles (including the provisions relating to principles 6 and 7 in Parts 4 and 5 of the Act)?

Q58 Should an anonymity and pseudonymity principle be added to the Privacy Act, either as part of principle 1 or as a separate principle? If so, what should be the content of such a principle?

Q59 Should the Privacy Act include an Openness principle? If so, what should be its content? If not, should openness be provided for in some other way?

Q60 Should any other new principles be included in the Privacy Act? If so, what are they?

CHAPTER 5 EXCLUSIONS AND EXEMPTIONS

Q61 We propose that the application of the privacy principles (not necessarily by way of the Privacy Act itself) to the House of Representatives and to MPs should be considered by a committee of Parliament. Do you agree?

Q62 We propose that the issue of extending the privacy principles to the parliamentary service bodies should be reviewed by a committee of Parliament at the same time as that committee considers the application of the principles to the House of Representatives and MPs. Do you agree?

Q63 We propose that the Ombudsmen should be made subject to the privacy principles. Do you agree?

Q64 We propose that the exclusion of the news media in relation to their news activities should remain in the Privacy Act. Do you agree?

Q65 We propose that the definition of "news activity" should remain as it is. Do you agree?

Q66 Do you think the definition of "news medium" should be amended to confine it to the print and broadcast media? Alternatively, should be it be confined to news media that are subject to a code of ethics and complaints procedure?

Q67 We propose that the limiting reference to Radio New Zealand and Television New Zealand should be removed from the definition of "news medium". Do you agree?

Q68 Are any other changes needed to the exclusions from the definition of "agency"?

Q69 Are any changes needed to section 55?

Q70 We propose that section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principle 9. Do you agree? Should the Commissioner be allowed to grant exemptions under section 54 from any other principles?

Q71 We propose that section 54 should continue to be limited to one-off exemptions only. Do you agree?

Q72 Are any other changes needed to section 54?

Q73 Should the meaning of "personal affairs" in section 56 be clarified? If so, how?

Q74 We propose that section 56 should be amended to provide that it does not apply where a person has collected information from an agency by engaging in misleading conduct (in particular, by falsely claiming to have the authorisation of the individual to whom the information relates or to be that individual). Do you agree?

Q75 We propose that section 56 should be amended so that it does not apply where personal information is obtained unlawfully (whether or not the person obtaining the information has been charged or convicted of a criminal offence). Do you agree?

Q76 We propose that section 56 should be amended so that it does not apply where the collection, use or disclosure of personal information results in identifiable harm to another individual. Do you agree? If not, do you support any of the other options discussed in paragraphs 5.53–5.55?

Q77 Do you have any other suggestions for amending section 56?

Q78 Should principles 1, 5, 8 and 9 apply to the intelligence organisations?

Q79 Should there be any other changes to the exemption for the intelligence organisations under section 57?

Q80 Should there be any changes to the procedures for investigating privacy complaints involving the intelligence organisations? Are any problems created by the dual jurisdiction of the Privacy Commissioner and the Inspector-General of Intelligence and Security?

Q81 Should any new exemptions be included in the Privacy Act?

CHAPTER 6 PRIVACY COMMISSIONER

Q82 Should section 13, or its heading, indicate that it is not an exhaustive list of the Privacy Commissioner's functions? Where should section 13 be located in the Act?

Q83 Do you have any concerns about the breadth of the Commissioner's functions? Should the functions be confined to matters involving informational privacy?

Q84 We suggest that the Privacy Act should express the Commissioner's functions in a more succinct way. Do you agree? How could this best be done?

Q85 We propose that sections 13(1)(d) and 21 should be deleted. Do you agree?

Q86 Are the reporting functions in section 13(1)(c), (p), (q) and (r) necessary? If so, is it necessary that the reports be to the Prime Minister?

Q87 Should any other functions in section 13 be removed?

Q88 We propose that a person or body other than the Privacy Commissioner should review the operation of the Act. Do you agree? If so, do you have any suggestions about who should conduct the reviews?

Q89 Should reviews continue to be required every five years?

Q90 We propose that there should be a requirement for the government to respond to reports arising out of reviews of the Act within a specified period of time. Do you agree?

Q91 We propose that the current audit power should be amended to give the Commissioner power to conduct mandatory audits, as outlined in paragraph 6.93. Do you agree?

Q92 Should any other functions be amended?

Q93 Do you think that the Commissioner should have any further functions or powers that we have not discussed?

CHAPTER 7 CODES OF PRACTICE

Q94 Are any changes to the Act required to make the development of codes of practice more effective, or to improve the effectiveness of codes generally?

Q95 We consider that codes of practice should be implemented by ordinary regulations approved by Cabinet, rather than simply being issued by the Privacy Commissioner. Do you agree?

Q96 Should reviews, or sunset provisions, be mandatory in relation to codes of practice?

CHAPTER 8 COMPLAINTS, ENFORCEMENT AND REMEDIES

Q97 We propose that the complaints, enforcement and remedies provisions of the Privacy Act should be reformed in the manner outlined in paragraphs 8.33–8.76. Do you agree? In particular do you agree that:

- the harm threshold in section 66 of the Act should be removed;
- the role of the Director of Human Rights Proceedings should be discontinued for privacy cases;
- for access reviews the Privacy Commissioner should determine the complaint and the role of the Human Rights Review Tribunal should be that of an appellate body;
- the Human Rights Review Tribunal should be chaired by a District Court Judge;
- the Privacy Commissioner should be given statutory power to issue enforcement notices; and
- non-compliance with an enforcement notice should be made an offence?

Q98 Are any other dispute resolution or enforcement mechanisms required?

Q99 Should the Act provide more specifically for the taking of representative complaints? If so:

- Should the representative be required to be personally affected by the alleged breach?
- Should the consent of other members of the group be required?
- Should the group be formed on an opt-in or opt-out basis?

Q100 Should there be new offences of:

(a) intentionally misleading an agency by impersonating an individual or misrepresenting the existence or nature of authorisation from an individual in order to obtain personal information or to have personal information used, altered or destroyed; and/or

(b) knowingly destroying documents containing personal information to which an individual has sought access in order to evade an access request?

Q101 Should the Act contain any further offences?

Q102 Are any changes needed to clarify the Ombudsmen's role in investigating the Privacy Commissioner's handling of complaints under the Privacy Act?

Q103 Do you have any further comments on the Act's provisions regarding complaints, enforcement and remedies?

Q104 Should there be greater openness about data mining by public agencies? For example, should public agencies be required to report annually on their data mining activities?

Q105 We consider that the current controls on information matching by public sector agencies are appropriate and should be retained. Do you agree?

Q106 We do not think that there is currently a case to impose detailed controls on information matching by private sector agencies. Do you agree? If not, can you provide examples of situations where a lack of controls has put people's privacy at risk?

Q107 We propose that Part 10 and Schedule 4 should be enacted as a separate Privacy (Public Sector Data Matching) Act. Do you agree?

Q108 We consider that all information matching undertaken by public sector agencies should require specific statutory authority, and be covered by the controls in Part 10 and Schedule 4. Do you agree?

Q109 We propose that the list of examples of what constitutes "adverse action" against an individual should be extended to include a decision to impose a penalty, and a decision to recover a penalty or fine imposed earlier. Do you agree? Should any other changes be made to the list of examples?

Q110 We are currently of the view that the definition of adverse action should not be amended to clarify that information matching programmes that have a beneficial consequence for individuals or no adverse consequence are expressly excluded. Do you agree?

Q111 We propose that the controls on information matching programmes by public sector agencies should be focused on computerised/automated matching, and manual matching should no longer be covered (computerised information matching with a manual component would continue to be covered). Do you agree?

Q112 We propose that the information matching guidelines in section 98 should be amended to require a mandatory protocol procedure so that the Privacy Commissioner has better information on which to assess proposals for new information matching authorities. Do you agree?

Q113 We propose that the period of notice that should be given by an agency before it takes adverse action against an individual on the basis of the results of an information matching programme should be increased from five working days to 10 working days. The Privacy Commissioner should also be empowered to shorten or waive the notice period in appropriate cases. Do you agree?

Q114 We propose that the Privacy Commissioner should be able to present a separate report to Parliament each year on his or her monitoring of information matching programmes, rather than include this in the Commissioner's annual report. Do you agree?

Q115 We propose that, in the absence of increased resources to enable the Privacy Commissioner to undertake the required 5-yearly reviews of information matching authorities under section 106, each authority should be sunsetted so that it expires after five years unless (a) renewed by Parliament, or (b) extended by Order in Council made on the recommendation of the Privacy Commissioner. Do you agree? If so, which option do you prefer?

Q116 We propose that, if the Privacy Commissioner continues to undertake reviews of information matching authorities, there should be a requirement on the Government to respond to the Commissioner's report within six months of the presentation of the report. Do you agree?

Q117 We propose that the Inland Revenue Department should no longer have a blanket exemption from the requirements to commence adverse action against an individual within 12 months, and to destroy personal information provided for or derived from an information matching programme once it is no longer needed. Specific exemptions for individual information matching authorities should be provided instead, if these can be justified. Do you agree?

Q118 We propose that the current information matching rules requiring publicity and notice of information matching programmes, and prohibiting the creation of separate databanks, should be stated in the body of the Act itself. Do you agree? Are any other information matching rules so important that they should also be included in the Act rather than a schedule?

Q119 Should the Act provide for the making of regulations amending the list of specified agencies in section 97 to ensure that the information matching controls in Part 10 continue to apply when agencies are reorganised?

Q120 Do you have any other comments or suggestions about information matching?

CHAPTER 10 INFORMATION SHARING

Q121 Are the principles set out in paragraphs 10.116–10.123 useful in framing a way forward for information sharing? Do you have any other suggestions?

Q122 We have presented the following mechanisms as possible means of regulating information sharing:

- guidelines;
- a code of practice;
- a national public sector information sharing strategy;
- a rebuttable presumption that personal information held by one public sector agency can be shared with other public sector agencies if such sharing is for the benefit of the individual concerned and is for a purpose that is broadly similar to that for which the information was obtained;
- allowing the Privacy Commissioner to issue binding or advance rulings;
- the enactment of a set of information sharing guidelines similar to the information matching guidelines in section 98;
- requiring greater openness about information sharing by public sector agencies (such as requiring them to report annually on their information sharing activities);
- the addition of a new "welfare" exception to principle 11;
- an extension of the current section 54 exemption power;

- a schedule of authorised information sharing activities;
- a new regime similar to the existing information matching regime; and
- a "common or integrated programme or service" exception.

What are your views on any of these mechanisms?

Q123 Do you have any other suggestions about how the sharing of information by public sector agencies might be facilitated in appropriate cases?

Q124 How should legal authority for sharing of personal information across borders between government agencies be provided for? How should the law ensure that privacy is protected when information is shared in this way?

CHAPTER 11 INTERACTION WITH OTHER LAWS

Q125 We propose that section 7 should be redrafted. Do you agree? Do you have any particular comments or suggestions for approaching this?

Q126 Do you think a published list or table of statutory provisions that override the privacy principles would be helpful? In what form should this be made available?

Q127 What presumptions or mechanisms should there be for clarifying the relationship between the Privacy Act and other legislation?

Q128 Should section 7 be redrafted to ensure that future delegated legislation does not override the Privacy Act except insofar as the empowering Act clearly so authorises?

Q129 Do you have any comments about the interaction of the privacy principles with the common law?

Q130 What are your views on whether there should be closer alignment of the tests for disclosure of personal information under the OIA and the Privacy Act?

Q131 Should the Privacy Act's deferral to the OIA be made explicit?

Q132 Should consideration be given to a specific right of review or complaints process for those affected by the release of personal information under the OIA?

Q133 Should consideration be given to formalising a consultation process between the public agency holding personal information and a person who may be affected by the release of that information under the OIA?

Q134 Should the OIA be able to be used by government agencies to obtain from each other information about individuals? If not, how should such a limitation be given effect?

Q135 Should consideration be given to combining all, or any parts, of the Privacy Act, the Official Information Act and the Public Records Act?

Q136 Do you have any preliminary views on umbrella regulation of privacy and freedom of information?

Q137 Do you have views about the current division of access rights between the Privacy Act and the OIA?

Q138 Do you have any views about the interrelationship between the Public Records Act and the Privacy Act, and between the Public Records Act and the privacy withholding ground in the OIA? Do you agree that the relationship between the different legislation should be clarified?

Q139 Should remedies be available to a person aggrieved by a decision to place personal information on open access in the Archives? If so, what kind of remedies?

Q140 Do you have any view about the question of jurisdiction for health information privacy as between the Privacy Commissioner and the Health and Disability Commissioner?

Q141 Do you have views about how privacy can be protected in relation to personal information used for statistical purposes?

Q142 Is a review of statutory secrecy provisions desirable?

Q143 Does the intersection of any other legislation with the Privacy Act require clarification or review?

CHAPTER 12 LAW ENFORCEMENT

Q144 Should section 27(1)(c) include more specific law enforcement grounds for the withholding of personal information about a requester? If so, which specific grounds should be included?

Q145 Would it be helpful if the Privacy Commissioner provided information or commentary about the law enforcement grounds for refusing access?

Q146 We believe that, as a result of the coming into force of the Criminal Disclosure Act 2008 and section 29(1)(ia) of the Privacy Act 1993, there is presently no need to make provision for limiting access by prisoners to information. Do you agree?

Q147 We suggest that the maintenance of the law exception should be redrafted for greater clarity. Do you agree?

Q148 Should there be separate maintenance of the law exceptions for the disclosure of personal information (i) to a law enforcement agency upon request, (ii) to a law enforcement agency in the absence of a request, and (iii) by a law enforcement agency?

Q149 Would it be helpful if the Privacy Commissioner provided information or commentary about the maintenance of the law exception to the use and disclosure principles?

Q150 Should Schedule 5 law enforcement information sharing continue to be dealt with in a specific Schedule to the Privacy Act? Alternatively, should this be dealt with in specific regulations, or in a specific code of practice?

Q151 Should additional transparency and accountability measures (like those that apply to information matching) also be applied to law enforcement information sharing? Alternatively, could Schedule 5 law enforcement information sharing be dealt with adequately under one or more of the generic information-sharing options outlined in chapter 10?

Q152 Is there any reason for Part 11 and Schedule 5 to continue to provide for local authorities to have access to any law enforcement information?

Q153 Should the power to amend Schedule 5 by Order in Council be reinstated? Should the power be subject to a sunset clause? What safeguards should be built into the process?

Q154 Should the maintenance of the law exception to the disclosure principle be redrafted to clarify that personal information may be shared between law enforcement agencies for law enforcement purposes? Should any other mechanism to facilitate information sharing between law enforcement agencies be considered?

CHAPTER 13 TECHNOLOGY

Q155 Do you have any comments on the role and functions of the Privacy Commissioner in relation to technological developments? Should the Privacy Commissioner's functions in relation to technology be revised and should any new functions be added?

Q156 Should the Privacy Act provide for a Privacy Advisory Panel, or empower the Privacy Commissioner to set up expert panels on particular issues, as the Australian Privacy Act does?

Q157 Is the basic framework of the Privacy Act adequate to deal with technological change? Should the privacy principles remain technologically neutral?

Q158 Do you have any comments about the role of privacy-enhancing technologies in government or the private sector, and how their use could be encouraged?

Q159 Should consideration be given to empowering the Privacy Commissioner to direct public or private sector agencies to produce Privacy Impact Assessments for new projects that may have a significant impact on the handling of personal information?

Q160 Do you have any comments about the privacy issues associated with the technologies discussed in this chapter? Is any particular law reform or regulatory response required in relation to any or all of these technologies? Should consideration be given to codes of practice or Privacy Commissioner guidelines in relation to any particular technology?

Q161 Do technologies not discussed in this chapter give rise to important privacy issues that require examination?

CHAPTER 14 TRANS-BORDER DATA FLOWS

Q162 Should there be more protections around personal information being sent out of New Zealand?

Q163 If you think there should be further reform, which of the approaches discussed in paragraphs 14.40-14.55 do you prefer? Would you prefer another model or variant not discussed here?

Q164 Does the Act require further amendments to implement the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy? Are any other amendments required in relation to cross-border enforcement cooperation?

Q165 Do you see value in implementing a cross-border privacy rules system in New Zealand? If so, do you have a view on the questions in paragraph 14.71?

Q166 Do you have any further comments on the issues raised by trans-border data flows?

CHAPTER 15 DIRECT MARKETING

Q167 Are any regulatory controls on direct marketing needed? If so, which forms of direct marketing require further controls:

- telemarketing;
- unsolicited mail;
- door-to-door marketing;
- autodialing;
- electronic spam;
- fax marketing;
- charitable solicitations;
- political donation solicitations; or
- other?

Q168 Which regulatory option or options do you favour:

- a direct marketing principle in the Privacy Act;
- a right to opt out of direct marketing in the Privacy Act, a Privacy Act code of practice, or regulations;
- a voluntary or compulsory Do Not Call Register for telemarketing; or
- any other option?

Q169 Do you have any comments about the privacy issues associated with online behavioural targeting? What, in your view, is the appropriate regulatory response to these issues?

Q170 Should the Privacy Act include a mandatory breach notification requirement, or is a voluntary notification model more appropriate?

Q171 How should a data breach be defined? Should a data breach notification requirement be applicable to all types of personal information, or should a more purposive definition be developed for the purposes of the breach notification regime?

Q172 In what circumstances should organisations be required to notify individuals that their personal information has been compromised? Should the legislation list the factors to be taken into account in deciding whether to notify? If so, what factors should the legislation list? Should there be different thresholds for notification to the individual and notification to the regulator?

Q173 Who should decide whether a notification must be made in response to a data breach?

Q174 Should the Privacy Commissioner have the power to compel an organisation to notify affected individuals?

Q175 In the case of a data breach should the agency be required to notify the Privacy Commissioner's Office? If so, should this be in every case, or only when the "notification threshold" is met?

Q176 Should other agencies be notified? If so, in what circumstances?

Q177 At which point should notification be required?

Q178 Should delays in notifying be allowed for law enforcement or any other purposes?

Q179 Should the method of notification be prescribed, or stated in terms of the objective to be achieved?

Q180 What information should have to be included in a breach notification?

Q181 What exceptions, if any, should be included in a data breach notification regime? In particular:

- Should encryption be an express exception or one of the matters to be included in the risk assessment exercise?
- Should public interest be included as a ground on which the Privacy Commissioner can waive an organisation's obligation to notify, or are more narrowly-defined exceptions more appropriate?

Q182 Is the complaints process an adequate mechanism for dealing with an organisation's failure to notify in the case of a data breach, or are further sanctions necessary?

Q183 Should it be decided that notification should be mandatory, do you agree that an amendment to principle 5, backed up by provisions later in the Act, is the best way to enact an obligation to notify? If not, how do you think the obligation should be enacted?

CHAPTER 17 IDENTITY CRIME	Q184	Are any changes needed, either to the Privacy Act or to other laws, to better address identity crime?
CHAPTER 18 PARTICULAR GROUPS	Q185	Are there any ways in which the Privacy Act or the Office of the Privacy Commissioner could better provide for the needs of Māori?
	Q186	Are there any ways in which the needs and concerns of particular cultural or religious groups in relation to privacy could be better met?
	Q187	Are any particular protections for young people required in relation to online privacy or direct marketing?
	Q188	Are any other new, specific protections for young people needed in the Act?
	Q189	Should the Act provide more specifically for when a child or young person should be treated as having capacity to exercise rights under the Act? If so, should there be a set age or a more individual test?
	Q190	Do you have any other concerns about the privacy of children and young people?
	Q191	Should the Privacy Act include any special provisions for adults with reduced capacity?
	Q192	Are there any other groups that have particular needs in relation to the Privacy Act? If so, how should these be provided for?
CHAPTER 19 HEALTH INFORMATION AND WORKPLACE PRIVACY	Q193	Is there a need for a separate review of health information and/or new health information legislation?
	Q194	Are you satisfied with the current legal framework governing workplace privacy, or is more specific regulation, such as a code of practice or specific legislation, needed to deal with workplace privacy issues?
	Q195	Do you have any other comments, or any further suggestions, about how the Privacy Act 1993 could be amended or improved?