LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

June 2011, Wellington, New Zealand | REPORT 123

REVIEW OF THE PRIVACY ACT 1993

REVIEW OF THE LAW OF PRIVACY STAGE 4

LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

E31 (123)

June 2011, Wellington, New Zealand | REPORT 123

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:

Honourable Sir Grant Hammond KNZM – President

Dr Warren Young – Deputy President

Emeritus Professor John Burrows QC

George Tanner QC

Professor Geoff McLay

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

New Zealand. Law Commission.

Review of the Privacy Act 1993 : review of the law of privacy, stage 4.

(Law Commission report ; 123)

ISBN 978-1-877569-14-2 (pbk.)—ISBN 978-1-877569-23-4 (internet)

1. New Zealand. Privacy Act 1993. 2. Privacy, Right of—New Zealand.

I. Title. II. Series: New Zealand. Law Commission. Report ; no. 123

342.930858—dc 22

ISSN 0113-2334 (Print)

ISSN 1177-6196 (Online)

This paper may be cited as NZLC R123

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

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

30 June 2011

Dear Minister,

NZLC R123 – REVIEW OF THE PRIVACY ACT 1993: REVIEW OF THE LAW OF PRIVACY STAGE 4

I am pleased to submit to you Law Commission Report 123, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4*, which we submit under section 16 of the Law Commission Act 1985.

Yours sincerely

Hon Sir Grant Hammond KNZM
President

FOREWORD

The Law Commission has been reviewing the law of privacy. The project was a very large one, and the Commission approached it in four stages. The first stage resulted in a study paper, *Privacy: Concepts and Issues*; the second in a report, *Public Registers*; and the third in a report, *Privacy: Penalties and Remedies*. The present report concludes stage 4. It is a review of the Privacy Act 1993, the Act which deals with the collection, security and use of people's personal information, and sets up the office of Privacy Commissioner.

The government has postponed action on stages 2 and 3 until the completion of this fourth stage, so that the proposed reforms can be seen as a package.

The review of the Privacy Act, the subject of this report, is timely. The Act is now 18 years old. In this modern age, technology, and its ability to gather, store and disseminate information about people, has advanced beyond anything imaginable in 1993. Much personal information is held by large agencies in both the public and private sectors. It can be sent to agencies overseas. It is very important to people that their personal information is properly protected, and that the law is flexible enough to be able to move with the times and provide that protection.

On the other hand, we must also accept that privacy is not an absolute value. It must be balanced against other important values: health and safety, law enforcement and national security, for example. The challenge is to get the balance right between protecting privacy and allowing disclosure of information to appropriate people when that is necessary.

This report investigates how far the Act's principles need to be amended. It also tackles some important policy questions, such as whether the Privacy Commissioner needs more powers; whether the complaints process, particularly in progressing claims to the Human Rights Review Tribunal, could be streamlined; whether agencies which lose people's information should have to tell them; and what the obligations should be of agencies which send personal information overseas.

These questions are important, not only for the citizens whose personal information is in question, but also for the agencies which deal with it.

In reaching its conclusions the Commission consulted with, and received submissions from, many persons and organisations. It records its thanks to all those who participated, and acknowledges in particular the assistance it has received from the Office of the Privacy Commissioner and the Ministry of Justice.

The Commissioners who worked on the privacy project were Sir Geoffrey Palmer and John Burrows. The legal and policy advisers who were involved in stage 4 were Ewan Lincoln, Joanna Hayward, Sara Jackson, Steven Melrose and Geoff Lawn. Legal and policy advisers who worked on other stages of the privacy review were Mark Hickford, Susan Hall, Rachel Hayward and Janet November.

Hon Sir Grant Hammond KNZM
President

Review of the Privacy Act 1993

Review of the law of privacy stage 4

CONTENTS

CHAPTER 6

CHAPTER 7

CHAPTER 8

CHAPTER 9

CHAPTER 10

CHAPTER 11

CHAPTER 12

APPENDICES

APPENDIX 1

APPENDIX 2

APPENDIX 3

APPENDIX 4

Glossary

This glossary contains a list of acronyms, abbreviations and other terms that are used regularly throughout this report, together with their corresponding meanings. Where appropriate, it also contains the names of some bodies and an explanation of what they do. It is followed by a list of sources that appear frequently in abbreviated form in footnotes, together with their full citations.

ALRC	Australian Law Reform Commission
APEC	Asia-Pacific Economic Cooperation. APEC is an Asia-Pacific regional economic and trade forum, consisting of 21 member economies.
Article 29 Data Protection Working Party	A Working Party set up under Article 29 of the EC Data Privacy Directive 95/46/EC. It is an independent European advisory body on data protection and privacy.
Commissioner	Privacy Commissioner (unless the context indicates otherwise)
Director	Director of Human Rights Proceedings
EU	European Union
Federal Trade Commission	The Federal Trade Commission is the Federal United States body which oversees consumer protection and competition in the United States, including the regulation of business practices that impinge on personal privacy.
HIPC	Health Information Privacy Code 1994
OECD	Organisation for Economic Cooperation and Development. The OECD is a forum of 34 member countries which promotes economic development.

OECD Guidelines	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
OIA	Official Information Act 1982
OPC	Office of the Privacy Commissioner (NZ)
PETs	Privacy-enhancing technologies (see chapter 10)
PIAs	Privacy impact assessments (see chapter 10)
PIPEDA	Personal Information Protection and Electronic Documents Act 2000. PIPEDA is the Canadian Federal privacy law that applies to the private sector.
Tribunal	Human Rights Review Tribunal or, prior to 2002, the Complaints Review Tribunal. The Human Rights Review Tribunal is established under the Human Rights Act 1993. It replaced the Complaints Review Tribunal, which existed from 1993 to 2002.

The following sources appear frequently in the footnotes to this report. They are cited in the footnotes as shown on the left below; the full citation appears on the right.

Enhancing National Privacy Protection	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, 2009).
For Your Information	Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008).
Issues Paper	Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC IP17, 2010).

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* (Wellington, 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* (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* (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* (Wellington, 2008).

Summary

INTRODUCTION

1 This report concludes the Law Commission's 4-stage Review of Privacy. This fourth stage is a review of the Privacy Act 1993, the Act which regulates the collection, security and use of people's personal information. We published an issues paper on the subject in March 2010, and this report follows that issues paper. Most of the recommendations in this report were foreshadowed in that earlier paper.

2 **Chapter 1**, **Introduction**, explains the background to, and history of, the review, and discusses the similar review recently completed in Australia. (We have referred to the Australian report frequently in this report.) This chapter also summarises briefly the main provisions of the Privacy Act. It concludes with a summary of the considerations we have borne in mind in our review: the need to keep the Act consistent with international privacy instruments; the need to ensure that it is able to keep pace with technological developments; the need to learn from the practical experience of working with the Act; and the need to remember that privacy is not an absolute value. The last of these considerations means that privacy must be balanced against other important values such as freedom of information, health and safety, law enforcement and the effectiveness of government and business.

THE ACT'S MAIN PROVISIONS

3 **Chapter 2**, **Scope, approach and key definitions**, gives an overview of the Act. The Act is principles-based, containing a series of 12 open-textured principles. Some of these principles are that people should know the purpose for which information about them is being collected; it should not be collected by unfair methods; once collected it should be kept secure; it should not be used or disclosed for purposes other than that for which it was obtained; and people should be allowed to access the information that an agency holds about them. To several of the principles there are a number of specific exceptions. We discuss the pros and cons of this approach. Open-textured language has the virtues of flexibility and capacity to move with the times. We conclude that these virtues justify retention of the principles-based approach, although we note also the downside: that application of the broadly-phrased language to a particular fact situation can sometimes be difficult, and can lead to misunderstandings and differences of opinion. We think that guidance and education for those applying the Act, together with some minor amendments to the principles, are a better solution than moving to a rules-based approach. In this chapter we also explain the role of guidance from the Office of the Privacy Commissioner (OPC).

4 We propose a new purpose section which, although based on the present long title of the Act, gives more emphasis to the fact that privacy is subject to exceptions which recognise other countervailing interests.

5 Chapter 2 also looks at some key terms and their definitions, and asks whether they need clarification or amendment. Some of the key terms used in the Act are "personal information"; "individual"; "collect"; and "publicly available publication". The open texture of which we spoke leads to the use of such expressions. The first two of these terms could do with guidance and explanation rather than amendment. In discussing "individual" we spend some time examining the vexed question of whether the Act should protect the privacy of deceased persons: currently it does not, with a number of specific exceptions. We think that only minor legislative change is merited, but that in some specific contexts codes of practice could be useful in making provision for information about deceased persons. But we think "collect" does need legislative amendment: currently it excludes unsolicited information, and this exclusion has caused uncertainty and ambiguity. We think that the definition of "publicly available publication" also needs amendment to keep up with this technological age; it must be clear that it includes publication on the internet. The rules about "publicly available publication" also need to be changed to avoid some of the anomalies that can exist at the moment.

6 **Chapter 3** is on the **Privacy principles**. The information privacy principles are at the heart of the Privacy Act. This chapter takes a detailed look at them to see if any of them, or the many exceptions to them, need amendment. Some of the amendments we propose are of a detailed nature, but they do involve some important questions. One such question is whether principle 4 (which provides that methods of collection must not be unlawful or unfair) should apply to *attempts* to collect information as well as to actual collection. One can well argue that if people try unsuccessfully to get information about someone by unfair and intrusive means, that individual's privacy can be invaded just as much as if personal information is actually obtained. There are also questions about people's rights to obtain access to their own information: whether anything can be done if they are coerced by another into requesting access; whether the likelihood of serious harassment should be a reason for refusing access; whether a request for access can be refused if the same information has been requested or refused before. One of the most important questions is whether the health and safety exception to the non-disclosure principle (principle 11) and the use principle (principle 10) should be relaxed. Currently the Act requires that for a threat to health and safety to justify disclosure of personal information, that threat must be "serious and imminent". It has been suggested frequently and forcefully that the word "imminent" is too strong: a threat to health and safety can still justify disclosing information even though the threat may not be likely to eventuate on the instant. We agree with that suggestion, and recommend that the word "imminent" be deleted, although in that case we think the word "serious" would benefit from definition. We also ask whether there should be any new principles, in particular one facilitating anonymity for people supplying information, or one advocating openness and transparency about information-handling practices. We support the first, but not the second.

7 **Chapter 4** is about **Exclusions and exemptions.** Some agencies are excluded from the coverage of the privacy principles; some activities are exempted from them. This chapter asks whether they should be. We conclude that the Parliamentary Service should be covered by the Act, but only in relation to its departmental holdings: information held by the Service on behalf of Members of Parliament should not be covered. But we suggest that Parliament itself may wish to consider the application of the privacy principles to other parliamentary entities.

8 The Ombudsmen are currently exempt from the Privacy Act. We acknowledge that the secrecy provisions of the Ombudsmen Act go much of the distance in protecting individual privacy, but believe there are still some residual areas where the Privacy Act could apply. We recommend that the Ombudsmen should be subject to the Privacy Act, in the interests of comparability with other organisations. We are satisfied that the specific provisions of the Ombudsmen Act will ensure that the security and efficiency of their investigations will not be compromised by their coming under the Privacy Act.

9 We think that the Office of the Auditor-General faces particular difficulties in its investigations, and that principles 6 and 7 of the Privacy Act (the access and correction principles) should not apply in respect of personal information held by the Auditor-General. We also believe that there should be an extension of the privacy principles which apply to the intelligence organisations, but that a proposal to create a general exception for access to intelligence investigatory material should await a review of the New Zealand Security Intelligence Service Act, rather than being dealt with in the present review.

10 The news media are largely exempt from the principles in the Privacy Act. We believe this exemption continues to be justified: the Act is so framed that some of it cannot be sensibly applied to the media, whose job is to provide information to the public. Nevertheless, it is clear that the media should respect privacy. We think the media regulators (the Broadcasting Standards Authority and Press Council) are the appropriate bodies to frame and enforce privacy principles which are sensible and workable in the media context. This leads us to propose that, for the purposes of the Privacy Act exemption, the term "news media" should be confined to media agencies which operate under a code of ethics and are subject to a complaints body. We also recommend the removal of the present anomaly that Television New Zealand and Radio New Zealand, while generally exempt from the Act's principles, are subject to principles 6 and 7, the access and correction principles.

11 The "domestic affairs" exemption in section 56 provides that information collected or held solely or principally for the purposes of personal, family or household affairs is exempt from the privacy principles. That is too absolute. We recommend that it be amended to ensure that objectionable conduct (say, publishing sensitive or humiliating information on the internet) is caught by the Act, even if that information was originally collected in a domestic context. We also recommend changes to section 54, which authorises the Privacy Commissioner to grant exemptions from some of the Act's principles.

ENFORCEMENT

12 We then proceed to examine how the Act's principles are enforced. With the exception of the access principle (principle 6) in relation to public sector agencies, the principles are not enforceable in a court of law: the Act is explicit about that. The Act sets up the office of Privacy Commissioner. If a person thinks he or she has been harmed by a breach of one of the Act's principles, he or she can lay a complaint with the Privacy Commissioner, who will then investigate the complaint and try to arrive at a settlement. If that attempt is unsuccessful, the case can go forward to the Human Rights Review Tribunal, which has an enforcement jurisdiction with the power to make orders and award damages.

13 The title of **Chapter 5, Role, functions and powers of the Privacy Commissioner**, is self-explanatory. We look at the way the Commissioner's functions are set out in the Act, and recommend abridgment and consolidation of the current very long list of Privacy Commissioner functions, although this is a question of drafting rather than getting rid of existing functions. The list of functions goes beyond hearing complaints: it includes monitoring, educational and reporting functions.

14 We also examine the current requirement that the Privacy Act be reviewed every five years and conclude that, given the rapid advance of technology which poses increasing threats for privacy, that review cycle should continue. But we think it should not be conducted by the Privacy Commissioner, as is currently the case. An independent review panel appointed by the Minister should perform the task.

15 Finally in this chapter, we discuss the Privacy Commissioner's code-making power. The Commissioner can make codes of practice to regulate particular activities or sectors. These codes have the force of law, and can vary the Act's principles. Currently there are three main ones, regulating the health sector, the telecommunications industry and credit reporting. We recommend that, while the power to make codes of practice is useful and should be retained, this important law-making power should not reside in the Privacy Commissioner alone as it does at the moment. Constitutionally, the present process is most unorthodox. Codes should be made by Order in Council on the recommendation of the Commissioner. Given that codes can vary an Act of Parliament and are therefore a particularly strong form of delegated legislation, we think the standard checks and balances should apply, although we acknowledge that there is no suggestion that the current process has in any way been misused.

16 **Chapter 6, Complaints, enforcement and remedies**, deals with the means of enforcement. Currently the "enforcement" system is complaints-based. The Privacy Commissioner investigates individual complaints, but has almost no enforcement powers; those powers reside in the Human Rights Review Tribunal.

17 The present processes have the potential to be complex and confusing. This is particularly so of the process of getting matters to the Tribunal, which currently involves the intervention of the Director of Human Rights Proceedings, who decides whether the case should proceed. We think there needs to be a streamlining and simplification of process, with the Commissioner able to take

a more direct role him- or herself. Moreover, a system centred on complaints by individuals is not always effective in correcting ongoing problems which may continue to affect others. We set out the principles which we think should underlie reform. They are based on cost-effectiveness, efficiency, speed of resolution, better means of ensuring systemic change, and a more effective range of enforcement tools.

18 First, we believe that the Director of Human Rights Proceedings should no longer have a role in privacy proceedings. The present process causes delay, duplication, and much confusion for the uninitiated. The Privacy Commissioner him- or herself should be able to take cases to the Tribunal.

19 Secondly, we recommend that complaints relating to access to one's own personal information under principle 6 should be able to be *determined* by the Commissioner (rather than, as at present, the Commissioner being able only to try to negotiate a solution). These cases can be dealt with on the papers: they are effectively *reviews* of an agency's decision rather than the investigation of a complaint of misconduct. The suggested system would be quicker and more efficient than the present one whereby, if the Commissioner fails to negotiate a solution, the matter goes to the Tribunal for a hearing. Under the proposed new system, appeals would lie to the Tribunal against a determination by the Commissioner.

20 Thirdly, we recommend that it be clarified in the Act that representative complaints (that is to say, complaints brought by one person on behalf of a group or class of affected persons) are possible under the Act. It could at times be a good thing for a class of persons who have all been affected by a breach of the Act to group together and be represented by one person. The Act also needs to provide detail about the rules applying to such complaints.

21 Fourthly, we recommend the creation of two new offences to add to the very small list of offences currently in the Act. One would deal with getting access to someone else's information by impersonating that person; the other with evading a request for access by destroying the relevant documents.

22 The fifth recommendation in this chapter is one of the most important in the report. It is that the Privacy Commissioner should be able to issue compliance notices: that is to say, notices requiring an agency to correct a practice which is not in compliance with the Privacy Act. The complaints system is not good at putting right continuing systemic problems, some of which can affect large numbers of people. We are persuaded that problem situations exist which could be corrected by the issue of a notice. A search of the statute books reveals a number of instances where other regulatory officials have similar powers. They are common in privacy regulators overseas. Compliance notices should be challengeable in the Human Rights Review Tribunal. If not challenged within a prescribed time, or if upheld by the Tribunal after challenge, non-compliance would be an offence. Compliance notices should be the exception rather than the rule: they should only be resorted to if persuasion has failed.

23 A sixth important recommendation is that the Privacy Commissioner should have power to require audit of an agency: essentially, an audit of its information-handling practices. There is already limited power to do this: the Commissioner must periodically review information matching programmes, and there is a requirement of audit in the Credit Reporting Privacy Code. Given the complex information-handling systems of some of the large organisations with which the Commissioner has to deal, and the limitations of the complaints system in dealing with systemic issues, we think a broader power to require audit of an agency is desirable. There is no intention that there be regular audits of all agencies; they should be undertaken sparingly and only where a good reason exists. They could be undertaken by the Commissioner, by a body commissioned to do so, or by the agency itself with a report to the Commissioner. They might be of only one aspect of the agency's operation.

24 Many overseas Privacy Commissioners have such a power. We note also that the Chief Archivist has, under the Public Records Act 2005, the function of conducting cycles of audits of the record-keeping practices of all public agencies: this Act is about information handling, just as the Privacy Act is.

25 **Chapter 7** is on the important topic of **Data breach notification**. "Data breach" is a term in very common use, grammatically inelegant though it may be. It refers to the situation where, due to a security lapse or deliberate hacking, personal information held by an agency is lost, or gets into the hands of unauthorised persons. Cases of large "spills" of personal data (often customer details) are frequently reported in the media. Currently, if there is such a breach, there is no obligation to notify the individuals concerned. When they eventually find out it may be too late for them to take protective measures. In some other jurisdictions there is an obligation to notify such breaches, and we examine whether there should be in New Zealand. We conclude that there should be, although the threshold should be set fairly high, given the potential resource implications: if even the most minor breaches had to be notified, the system would break down under its own weight. We conclude that there should be an obligation to notify (a) if doing so would enable the individuals concerned to take preventive measures, for example by cancelling their credit cards or changing their passwords; or (b) if the breach is a *serious* one: we propose criteria for making that judgment. The chapter also discusses the detail of the statutory provisions which would be needed were such a duty to be imposed: they would cover such questions as who should notify; how and when notification should take place; whether the Privacy Commissioner should also be told; and whether there should be any exceptions to the duty.

MISCELLANEOUS

26 The last five chapters cover a range of matters.

27 **Chapter 8**, **Interaction with other laws**, notes that the Privacy Act interacts with a number of other statutes. Sometimes that interaction is quite complex, and there can be questions about which statute prevails in the case of inconsistency. (This problem is not peculiar to the Privacy Act: it is an inevitable consequence of our New Zealand system of legislation, which does not have a "seamless" code.)

28 This chapter recommends a redrafting and simplification of section 7, which essentially provides that in the event of inconsistency between the Privacy Act and another law, the other law prevails. At the moment, section 7 is extremely complex. We also recommend that the Legislation Advisory Committee Guidelines should contain guidance that future Acts should expressly indicate their relationship with the Privacy Act, where that relationship is likely to be an issue. It would be helpful if the Office of the Privacy Commissioner and the Ministry of Justice could provide a list of frequently-arising statutory overrides of the Privacy Act.

29 In addition, we look at a number of instances where specific legislation has given rise to particular problems in its relationship to the Privacy Act. The main ones are as follows. The relationship between the Privacy Act and the privacy withholding ground in the *Official Information Act 1982* has been productive of some uncertainty in agencies which have to apply both Acts. We propose a provision which clarifies that, when a request is made under the Official Information Act, it is that Act which prevails. The interface between the Privacy Act and the *Public Records Act 2005* is also less straightforward than we think desirable, and we recommend some amendments to clarify that relationship. We also discuss the interaction between the Privacy Act and some legislation governing criminal records: *the Criminal Disclosure Act 2008*, *the Evidence Regulations 2007* and the *Criminal Proceedings (Access to Court Documents) Rules 2009*. Most importantly, we ask whether the obligation to disclose relevant information to a defendant under the Criminal Disclosure Act should be subject to an exception where the disclosure would involve an unwarranted intrusion into the affairs of a third person. (Our concern arises from a case where a prosecution disclosure involved details of a large number of a website's customers who had nothing to do with the alleged offence.) We conclude that the Act should contain an express reference to the interests of third persons in determining what information is "relevant".

30 **Chapter 9** discusses **Law enforcement**. "Maintenance of the law" is an exception to the principles of the Privacy Act in two quite distinct situations:

(i) It is an exception to the duty to *give an individual access* to his or her own personal information.

(ii) It is an exception to the duty *not to disclose* an individual's personal information to others.

31 There is some uncertainty as to what the exception means. It is another open-textured term. But it is in common use throughout the statute book, and it will not be easy to amend it significantly without creating ramifications downstream. We recommend that further guidance be made available as to what it means and how it should be applied. But we think there should be a few statutory amendments. The most important relates to the reporting of offences. The Police have a particular concern that citizens are reluctant, because of the Privacy Act, to report offending to them. We think there should be a new exception spelling out expressly that the reporting of suspected offences is permitted under the Privacy Act. An information campaign on this subject would also be worthwhile.

32 In this chapter on law enforcement we also discuss schedule 5, the law enforcement schedule. If our proposals on information sharing (see appendix 1) are accepted, schedule 5 will simply merge into the new system that we propose for information sharing: it will, in other words, be overtaken by events.

33 **Chapter 10, Technology**, emphasises the challenges to privacy posed by advances in technology. We summarise some of the main areas: for instance, the internet, online tracking and targeted advertising, cloud computing, deep packet inspection, location and tracking technologies, and biometrics. All of these can have privacy implications, and things are moving very fast. The question is whether the Privacy Act needs to be amended to take account of this rapidly changing landscape. Overall, we think the broad principles of the Act are flexible enough to cope. But it should be made clearer than it currently is that the Privacy Commissioner's watching brief over privacy in general is broad enough to ensure that he or she can monitor all technological developments and not just those relating to computers: a small amendment will achieve that.

34 We encourage the establishment by the Commissioner of expert committees to assist, and also to promote privacy by design (that is, the use of privacy-enhancing technologies in new products).

35 We also believe that there should be a requirement for public sector agencies to do privacy impact assessments when undertaking new developments which could affect privacy, although we think that should best be provided for in a policy decision communicated in a Cabinet Office Circular rather than by a legislative amendment. We recommend that in respect of one new technology – biometrics – the Privacy Commissioner should explore the possibility of a code of practice.

36 We also note the critical importance of educating people – particularly young people – on how to respect and protect their online privacy.

37 **Chapter 11** is about **Sending personal information overseas**. These days, information is truly an international commodity. So is privacy protection: not only do international organisations have privacy principles (OECD, EU and APEC, for example) but there is an international community of privacy commissioners and other regulators who sometimes need to cooperate to discourage privacy-intrusive practices by multinational enterprises.

38 In this chapter we are concerned with the transmission of personal information to an entity outside New Zealand. This may be by way of outsourcing, or for some other purpose. By "outsourcing", we mean situations in which the information is held, stored or processed by the other agency for the "outsourcer", or where the relationship is essentially a principal-agent relationship. We recommend that, in relation to outsourcing-type activities, there should be a statutory requirement that the New Zealand agency which has outsourced the information should be absolutely accountable if anything goes wrong. It has employed someone else to do its job, and it should be just as if it continued to hold the information itself. There is such a provision in the Act now, but it needs to be made clearer. (The same principle should also apply if the outsourcing arrangement is entirely within New Zealand.)

39 As to other sorts of transfer of information overseas (assuming the transfer is itself permitted under the privacy principles) we recommend that there should be an obligation of due care and diligence on the part of the New Zealand transferor to ensure that the overseas recipient is able and willing to observe acceptable privacy standards. The Privacy Commissioner should play a part by maintaining a list of privacy frameworks which are acceptable for this purpose.

40 There have been some striking instances recently where the Privacy Commissioners of several countries have joined together to try to put pressure on multinationals to desist from privacy-invasive practices. The Act should enhance the Privacy Commissioner's power to cooperate with overseas Privacy Commissioners and similar regulatory authorities. Limited power was given in a 2010 amendment, but it needs to be strengthened. The Act should also contain a mechanism to allow for the recognition of systems of regional cross-border privacy rules at some future stage, should present APEC initiatives for such rules proceed.

41 In **Chapter 12** we consider some **Other issues**. Although a miscellany of matters is dealt with in this chapter, their importance should not be underestimated.

42 In the section on *culture and privacy* we particularly discuss areas in which Māori and Pākehā views of privacy may be different. We consider how we can better ensure that the perspectives of different cultures are taken into account and given effect to by the Privacy Commissioner. We propose the inclusion of a provision in the Privacy Act to facilitate that. The provision we prefer is one drawn from the Families Commission Act. *Children and young people* raise special questions too. We have debated whether to make special provision in relation to children, and in particular whether there should be an "age of authorisation" (say 16) at which young people can validly give their consent to the collection, use or disclosure of their information. But, due to the difficulties of verifying age online (which is where most of the problem is), and given OPC's view that the law is workable as it stands, we have opted for minimal change. We have, however, proposed that age should be a factor in deciding whether collection practices are "unfair" for the purpose of privacy principle 4. We also support express reference in section 14 to New Zealand's international obligations concerning the rights and best interests of the child.

43 We also recommend the formation of a working group to consider issues of capacity under the Privacy Act.

44 *Direct marketing* is a recurring topic in discussions of privacy. Intrusive marketing practices can upset people. In our view this is as much a matter of consumer law as of privacy. We are attracted to the idea of putting the "do not call" register currently operated by the Marketing Association on a statutory basis, and suggest that the Ministry of Consumer Affairs should progress this work. It seems to us that an amendment to the Fair Trading Act would be the appropriate vehicle.

45 Unique identifiers have been subject to special provision since the commencement of the Privacy Act. We examine them in a discussion of *identity crime*, and recommend that agencies which display unique identifiers must take all reasonable steps – such as number truncation – to minimise the risk of misuse.

46 *Health privacy* is a sensitive and very complex issue. It may be necessary for health professionals to share an individual's health information, and health information (usually anonymised) can be important for research purposes. Yet no other kind of information is as "private" and sensitive as health information. Currently, the law about it is contained in a number of Acts, and in the Health Information Privacy Code. We believe the area requires specific and specialist study, and that the rules should be codified in a separate statute. Such a statute would go wider than privacy: it would be a health information statute.

47 We asked in our issues paper whether there needs to be specialist provision for *workplace privacy*: we put forward the possibility of a separate Workplace Privacy Act. While concerns were certainly expressed in submissions about intrusions on employee privacy, there was insufficient support for a separate Act. But some of the proposals for amendments to the Privacy Act which we recommend in this report address concerns in the context of the workplace just as much as elsewhere.

INFORMATION SHARING AND MATCHING

48 The report contains two appendices on the subjects of **Information sharing** and **Information matching**. Our issues paper contained chapters on those topics. The first of them is about the ability of government agencies to share personal information about individuals. Such sharing may be with a view to providing better and more efficient services for individuals and families. It may be with a view to detecting wrongdoing. It may, indeed, be for any of a large number of purposes. But such arrangements do have significant implications for the privacy of the individual. Currently, attempts to share information do not always work satisfactorily, with agencies taking different views as to what the law will permit. This question is of considerable interest to the Government, and the Minister Responsible for the Law Commission asked the Commission to publish its conclusions on information sharing in advance of our final report on the review of the Act. We did so on 29 March 2011, in the form of a Ministerial Briefing. This was published on our website on the day it was presented to the Minister. It is currently under consideration by the Government. We publish it in this report as **appendix 1**.

49 In essence, our view is that proposals for the sharing of personal information between government agencies should be drawn up as agreed programmes, go through a process of consultation which will include consultation with the Privacy Commissioner, and be submitted for final approval by Order in Council. The purpose would be to ensure that there was certainty as to what information could be shared, while still ensuring that risks to privacy are properly managed. A new part of the Privacy Act would lay down the process. It would contain a statement of matters which would need to be covered in each programme agreement, and the criteria for approval. It would also prescribe transparency requirements: approved programmes would need to be published, a list of them should be contained in a schedule to the Privacy Act, and there should be reports on their operation. The appendix also discusses some important questions, such as whether non-governmental organisations should come within the scope of this sharing regime, and whether *all* sharing programmes between government agencies should require approval, or only those which involve variation of the Privacy Act's principles.

50 Another question is what will happen to information matching if our proposals about information sharing are accepted. In our view, information matching is just a subset of information sharing, and it is a subset which is very hard to define with precision. Since the inception of the Privacy Act, information matching has been dealt with by a special statutory regime in the Act. Matching programmes are authorised individually by special statutory provisions, and once in place are subject to strict reporting and monitoring requirements. It is our view that if government accepts our information sharing proposals, information matching should simply merge into those, and be subject to the new rules about information sharing. But, in case our proposals on information sharing are not accepted and the information matching rules stay in the Act, we set out in **appendix 2** our recommendations for some (relatively technical) amendments to those rules.

Summary of recommendations

CHAPTER 2

R1 A new Privacy Act should be enacted. In addition to implementing the recommendations of this report, it should incorporate changes recommended by the Privacy Commissioner in *Necessary and Desirable* and its supplements.

R2 The Privacy Act should continue to take an open-textured, principles-based approach to regulating information privacy.

R3 The Privacy Act should have a purpose section, which should state that the purposes of the Act are to:

- promote and protect privacy of personal information, subject to exceptions and exemptions which recognise other rights and interests that will sometimes override privacy;
- provide for access by individuals to their personal information that is held by agencies, and for correction of such information;
- provide remedies for interferences with privacy of personal information;
- give effect to internationally-recognised privacy obligations and standards, including the OECD Guidelines; and
- make other provision for the protection of individual privacy.

R4 The definition of "personal information" should not be amended, but the Office of the Privacy Commissioner should develop guidance with respect to the "identifiable" element of the definition.

R5 The Privacy Act should provide that codes of practice may apply any of the privacy principles to information about deceased persons.

R6 Causes of action under the Privacy Act should survive the complainant's death, for the benefit of his or her estate. A "cause of action" should be defined as accruing at the time the requirements of section 66 of the Act are met.

R7 The definition of "collect" should be amended to provide that situations in which an agency has taken no active steps to acquire or record information are excluded from the definition.

R8 The definition of "publicly available publication" should be amended to make it clear that:

- it includes websites and other material published in electronic form;
- a publication can be publicly available even if a fee is charged for access; and
- public registers are included only to the extent that they are generally available to the public, by moving the reference to "a public register" from the end of the definition, so that it appears instead before the words "or other publication".

R9 The Office of the Privacy Commissioner should develop guidance material with respect to the meaning of "publicly available publication", focusing particularly on information to which access is restricted to some extent.

R10 The scope of the "publicly available publication" exceptions to principles 10 and 11 should be narrowed, so that the exceptions cannot be relied on if, in the circumstances of the case, it would be unfair or unreasonable to use or disclose personal information obtained from a publicly available publication.

CHAPTER 3

R11 The word "directly" should be deleted from principles 2(1) and 3(1).

R12 Principle 2(2) should be amended by adding a new exception covering situations in which an agency believes, on reasonable grounds, that non-compliance is necessary to prevent or lessen a serious threat to the health or safety of any individual.

R13 Principles 3(4)(a) and 3(4)(f)(ii) should be deleted.

R14 Principle 4 should be amended to make it clear that it applies to attempts to collect information.

R15 The Privacy Commissioner should develop guidance material with respect to principle 5 and the issue of employee "browsing" of personal information.

R16 Principle 8 should be amended so that it clearly applies to both use and disclosure.

R17 Section 45 should be amended to provide that an agency shall not give access to information requested under principle 6(1)(b) if the agency has reasonable grounds for believing that the individual concerned is making the request under duress in the form of actual or threatened physical harm or psychological abuse.

R18 Section 66(2) should be amended to provide clearly that failure by an agency to comply with the requirements of section 45 is an interference with privacy.

R19 "Authorise" should be defined in section 2 as excluding situations in which an individual's agreement is obtained under duress in the form of actual or threatened physical harm or psychological abuse.

R20 Where an agency is not willing to correct personal information in response to a request made under principle 7, the agency 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.

R21 Sections 27 to 29 should be amended to incorporate the agency "belief on reasonable grounds" threshold, for consistency with principles 10 and 11.

R22 Section 27(1)(d) should be amended so that an agency may refuse access if disclosure of the information would be likely to present a serious threat to public health or public safety, or to the life or health of any individual.

R23 A new provision should be added to section 29, allowing agencies to refuse access where disclosure of the information would create a significant likelihood of serious harassment of an individual.

R24 The Office of the Privacy Commissioner, in consultation with the Ombudsmen, should develop guidance material in relation to access requests involving mixed information about the requester and other individuals.

R25 A new provision should be added to section 29, allowing agencies to refuse access where disclosure of the information requested:

- would involve disclosure of information about another individual or a deceased individual who is a victim of an offence or an alleged offence; and
- the disclosure would be likely to cause significant distress, loss of dignity or injury to the feelings of that victim or of a deceased victim's family if they were to learn of it.

R26 Section 29(1)(c) should be amended to add "or relevant health practitioner" after "medical practitioner". Section 29(4) should be amended to define "health practitioner" as having the same meaning as in section 5(1) of the Health Practitioners Competence Assurance Act 2003, and "relevant health practitioner" as "a health practitioner whose scope of practice includes the assessment of an individual's mental state".

R27 A new provision should be added to section 29, allowing agencies to refuse access if the same information, or substantially the same information, has previously been provided to the requester, or has previously been denied to the requester in accordance with one of the grounds for refusal, provided that no reasonable grounds exist for the individual to request the information again.

R28 Section 35(3)(b)(i), which provides that an agency that is not a public sector agency may charge for correction of personal information, should be deleted.

R29 Complexity of the issues raised by a personal information request should be added to the grounds in section 41(1) on which an agency may extend the time limit for responding to a request.

R30 The words "and imminent" should be deleted from principles 10(d) and 11(f).

R31 The Act should set out criteria for assessing seriousness for the purposes of the existing health and safety exceptions to principles 10 and 11, as well as for the new health and safety exception to principle 2 and the new health and safety ground for refusing access in section 27 (see R12 and R22 above). These criteria should be the likelihood, consequences and imminence of any threat to health or safety.

R32 Principle 12(2) should be redrafted so that the meaning of "assign" is clearer.

R33 An exception for the use of unique identifiers for statistical and research purposes should be added to principle 12(2).

R34 The Office of the Privacy Commissioner should develop guidance material on compliance with principle 12(4), aimed at agencies that routinely ask customers or clients to provide identification.

R35 Principle 1 should be amended by adding a new sub-clause providing that individuals should be able to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do so in the circumstances.

CHAPTER 4

R36 The Privacy Act should apply to the Parliamentary Service, but only in respect of its departmental holdings. Information held by the Parliamentary Service on behalf of Members of Parliament should not be covered by the Privacy Act.

R37 The Ombudsmen should be deleted from the list of entities excluded from the definition of "agency".

R38 The definition of "news medium" should be amended so that the news media exclusion from the Privacy Act applies only to media that are subject to a code of ethics that deals expressly with privacy, and to a complaints procedure administered by an appropriate body.

R39 The limiting reference to Radio New Zealand and Television New Zealand should be removed from the definition of "news medium", and consequentially section 29(1)(g) should also be deleted.

R40 Section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principles 9 and 12.

R41 Section 54 should be amended to require the Privacy Commissioner to report annually on exemptions applied for and granted under section 54, and to maintain on the Commissioner's website a list of all current exemptions.

R42 Section 55 should be amended to provide that principles 6 and 7 do not apply in respect of personal information held by or on behalf of the Auditor-General, and in connection with the Auditor-General's statutory functions. The provision should make clear that principles 6 and 7 still apply to personal information about the Auditor-General's current, former and prospective staff.

R43 Section 56 should be amended to state expressly that the exemption applies to all of principles 1 to 11.

R44 Section 56 should be amended to provide that it applies to information collected or held "solely" (rather than "solely or principally") for the purposes of, or in connection with, personal, family, or household affairs.

R45 Section 56 should be amended to provide that it does not apply where:

- an individual 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);
- personal information is obtained unlawfully (whether or not the individual obtaining the information has been charged with or convicted of a criminal offence) – this includes the collection of information by unlawful means, and the use or disclosure of information obtained by unlawful means; or
- the collection, use or disclosure of personal information would be highly offensive to an objective reasonable person.

R46 Section 57 should be amended to provide that principles 1, 5, 8 and 9 apply to the intelligence organisations, in addition to principles 6, 7 and 12 as at present.

CHAPTER 5

R47 Section 13 should be amended to make it clear that it is not a complete list of the Privacy Commissioner's functions.

R48 Section 13(1)(d) and section 21 should be repealed.

R49 The Privacy Act should contain a provision that it is to be reviewed every five years. The review should be undertaken by a committee appointed by the Minister, and containing persons expert in privacy, law and technology.

R50 The Government should be required to table in Parliament within six months a response to each review of the Act.

R51 The list of the Privacy Commissioner's functions in the present section 13 should be abridged and consolidated as set out in paragraph 5.28.

R52 Codes of practice should continue to be developed by the Privacy Commissioner, but should require approval by the Governor-General in Council.

R53 The Governor-General in Council should be able to reject a proposed code, but not to amend it. If a code is rejected, the Minister should provide reasons to the House of Representatives.

CHAPTER 6

R54 The harm threshold in section 66 should remain in relation to complaints.

R55 The role of the Director of Human Rights Proceedings should be removed in privacy cases. The Privacy Commissioner should decide which cases are to proceed to the Human Rights Review Tribunal and act as the plaintiff in those cases, and perform the other roles currently performed by the Director.

R56 The Privacy Commissioner should be able to finally determine access complaints under principle 6 and issue a notice to release the information.

R57 Compliance with a notice to release information (as referred to in R56) should be able to be enforced by order of the Human Rights Review Tribunal.

R58 A determination under principle 6 should be appealable to the Tribunal.

R59 If a complainant seeks damages for failing to obtain access to information, he or she should file a separate claim which would be heard by the Tribunal after a determination by the Privacy Commissioner.

R60 The Privacy Act should specifically provide that representative complaints are permitted, and provide more detail about them. It should provide that:

- the representative need not be personally affected;
- complaints to the Privacy Commissioner should be on an opt-out basis; and
- if the matter proceeds to the Tribunal, the Chairperson should determine who should be notified and whose consent should be required.

R61 The chairperson of the Human Rights Review Tribunal should be a judge at the level of a District Court Judge.

R62 The Human Rights Review Tribunal should not be empowered to order exemplary damages.

R63 The Privacy Commissioner should have power to issue compliance notices. The Act should provide as follows:

- The power should lie in relation to breaches of the information privacy principles or any other statutory duty imposed by the Act.
- The matters to be taken into account before making an order should include:
  - other possible means of securing compliance;
  - whether the agency has been cooperative;
  - the likelihood of recurrence;
  - the number of people who might be affected by the breach; and
  - the extent of the non-compliance.
- Notices should be able to be issued in relation to matters discovered as the result of a complaint or in any other way.
- The agency should have the right to be heard before the issue of a notice.
- There should be a right to challenge the notice in the Human Rights Review Tribunal.
- If the right of challenge is not exercised the notice should become enforceable; if the right of challenge is exercised and does not succeed, the Tribunal should issue an enforcement order.
- The Commissioner should have a discretion to publish the fact that a notice has been issued.
- Non-compliance with an enforceable notice should be an offence under the Privacy Act.

R64 The Privacy Commissioner should have power to require audits of agencies. This power should have the following features:

- The Privacy Commissioner should have power to undertake such audits personally; to commission another organisation to do so; or to require an agency to conduct a self-audit and report the results to the Commissioner.
- The Privacy Commissioner should have power to require an audit for good reasons. Among the good reasons might be:

(a) that there are reasonable grounds to believe that an agency's systems are not adequate to protect privacy;
(b) that an agency or agencies are involved in the handling of particularly sensitive information (for example, health information); and
(c) that an agency is engaging in a new and relatively untested practice (such as biometric testing).

- The power of mandatory audit should apply to both the public and the private sectors.
- The Privacy Commissioner should have appropriate powers to investigate, question persons and require information.
- The report on an audit should be given to the agency in question, but there should be power in the Privacy Commissioner to publish the findings more widely.

R65 The Privacy Commissioner should issue a protocol of the processes to be followed for conducting an audit.

R66 There should be new offences of:

(a) Intentionally misleading an agency by impersonating an individual or misrepresenting an authorisation from an individual in order to obtain that individual's personal information, or to have that information used, altered or destroyed.
(b) Knowingly destroying documents containing personal information to which a person has sought access.

CHAPTER 7

R67 Data breach notification should be mandatory, but only in clearly confined circumstances.

R68 The criteria for notification should be:

(a) if such notification will enable the recipient to take steps to mitigate a real risk of significant harm; or
(b) if the breach is a serious one.

R69 In determining whether a breach is serious the agency should take into account:

(a) whether or not the information is particularly sensitive in nature;
(b) the hands into which it may fall or have fallen;
(c) whether it is reasonably foreseeable that significant harm might result; and
(d) the scale of the breach.

R70 The responsibility to notify should lie on the agency which held the information for the purposes of principle 5 and from whose control it has escaped.

R71 Individuals whose information has been compromised should be notified. The Office of the Privacy Commissioner should also be notified.

R72 The Privacy Act should provide that the Office of the Privacy Commissioner will not publish the identities of agencies which notify breaches, unless the agencies consent or unless in a particular case the public interest so requires.

R73 Notification should be made as soon as reasonably practicable, with an exception where an investigation by a law enforcement agency might thereby be prejudiced.

R74 The notice should be such as to fully and fairly inform the individual, and, where practicable, to point out steps the individual could take to mitigate loss.

R75 Notification should be to the individual where possible, with provision for substituted service.

R76 There should be an exception to the requirement of notification where it would be contrary to the public interest.

R77 Failure to notify should be a ground of complaint to the Privacy Commissioner. The Privacy Commissioner should also have power to issue a compliance notice.

R78 The obligation to notify should be enacted as part of principle 5, with more detailed provisions elsewhere in the Privacy Act.

R79 If data breach notification becomes compulsory, the Privacy Commissioner should publish guidance on the subject.

CHAPTER 8

R80 Section 7 should be repealed and replaced by a new provision. That provision should:

- be headed "Relationship to other enactments";
- provide that in case of inconsistency between a privacy principle and another Act, the other Act will prevail;
- provide that regulations previously made which prevail over the privacy principles should continue so to prevail; and
- provide that in future regulations should not override the privacy principles unless the empowering Act expressly so provides.

R81 Section 7(5) should be moved to Part 6 of the Act.

R82 Section 7(6) should be moved to Part 7 of the Act, should such a provision remain necessary.

R83 The Legislation Advisory Committee Guidelines should contain a guideline that new legislation with privacy implications should, where possible and appropriate, expressly indicate the relationship between the Privacy Act and the new Act.

R84 The Legislation Advisory Committee should consider re-examining its guidelines on relationships between Acts to see whether more examples and guidance might be given.

R85 The Office of the Privacy Commissioner and the Ministry of Justice should consider issuing a list of frequently-arising statutory overrides of the Privacy Act.

R86 An exception should be added to principle 11 making it clear that when requests for personal information are made to agencies subject to the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, the latter Acts govern such requests (except in relation to requests by individuals for access to their own personal information).

R87 The Public Records Act 2005 should require the Chief Archivist to consult the Privacy Commissioner when preparing standards about access to archived records.

R88 A subsection should be added to section 18 of the Public Records Act expressly providing that that section prevails over principle 9 of the Privacy Act.

R89 Section 16 of the Criminal Disclosure Act 2008 should contain a provision that, in deciding whether information is relevant for the purpose of section 13(2) of that Act, consideration must be given to the extent to which it relates to the private affairs of another individual.

R90 The Evidence Regulations 2007 should expressly provide that they apply to the exclusion of privacy principles 6 and 7.

R91 Section 42(2) of the Criminal Disclosure Act 2008 should be amended to refer to the Evidence Regulations 2007.

R92 Statutory secrecy provisions should be addressed in:

(a) the list of provisions overriding the privacy principles that we suggest be prepared by the Office of the Privacy Commissioner and the Ministry of Justice (R85); and

(b) the enhanced discussion in the Legislation Advisory Committee Guidelines of relationships between Acts (R83 and R84).

CHAPTER 9

R93 Section 27(1)(c) should be amended to clarify that the access refusal ground is concerned with protecting the maintenance of the law by public sector agencies.

R94 The Ministry of Justice should coordinate with the Privacy Commissioner and the Ombudsmen on the development of guidance or commentary on the maintenance of the law as a ground to refuse or withhold the provision of information. The commentary or guidance should cover use of the provision in the Privacy Act, the official information legislation and the Criminal Disclosure Act.

R95 Should it not be possible to produce coordinated guidance in the short term, the Privacy Commissioner should develop independent guidance on the maintenance of the law access refusal ground in the Privacy Act in consultation with the Ministry of Justice and the Ombudsmen.

R96 The Privacy Commissioner should develop an information sheet or guidance on the maintenance of the law exception to principle 11. This should include guidance on responding to law enforcement requests for information and an explanation of the steps an agency should take to assure itself of the necessity for the disclosure. As part of this work, the Privacy Commissioner should consult with law enforcement agencies about the form and process for making requests for information under the Privacy Act.

R97 A new exception to principle 11 should be created that would expressly permit an agency to report any reasonably held suspicion or belief that an offence has been or may be committed, including any relevant information about that offence, to a public sector agency with law enforcement functions.

R98 The Privacy Commissioner and the Police should consider working collaboratively on an information campaign about the reporting of crime under the Privacy Act.

R99 Further to proposal 5 in Appendix 1, Part 11 of the Privacy Act should be repealed, subject to transitional provisions to grandparent law enforcement information sharing arrangements that are currently contained in Schedule 5.

R100 Access to public registers such as the driver licence and motor vehicle registers should be dealt with under the relevant statute authorising the particular register.

CHAPTER 10

R101 Section 13(1)(n) should be amended to delete the word "computer."

R102 The technology-neutral privacy principles should be retained. However, during this period of rapid technological change, the principles should be regularly reviewed (5-yearly) to ensure that the Privacy Act continues to effectively respond to privacy issues raised by technological developments.

R103 The Privacy Commissioner should consider convening an expert Privacy by Design Panel to promote privacy by design and to raise awareness of privacy-enhancing technologies.

R104 The Government should adopt a policy and issue a Cabinet Office circular setting out the circumstances in which public sector agencies are expected to produce a privacy impact assessment.

R105 The State Services Commission should provide guidance on its website as to expectations for use of privacy impact assessments in the public sector, such guidance being prepared in consultation with the Department of Internal Affairs and the Privacy Commissioner.

R106 The Privacy Commissioner should consider whether it is timely to issue a code of practice or guidance covering biometrics.

CHAPTER 11

R107 The Privacy Act should include an express statement of full accountability for cross-border outsourcing arrangements. It should be based on the first part of the Canadian Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) provision to the following effect:

> An agency is responsible for personal information it holds, including information that has been transferred to a third party for storage, custody or processing.

R108 The Privacy Commissioner should provide guidance for agencies on conducting risk assessment prior to outsourcing personal information overseas and on the use of contractual or other means to ensure the application of privacy standards of a kind comparable to the New Zealand Privacy Act.

R109 The Privacy Act should include an express statement of full accountability for domestic outsourcing arrangements, as a parallel provision to that recommended in R107.

R110 A new accountability measure should be introduced for disclosures of personal information overseas (other than outsourcing arrangements). Disclosing agencies should be required to take such steps as may be reasonably necessary to ensure that the information disclosed will be subject to acceptable privacy standards.

R111 Exceptions to the new measure should include disclosures:

- to the individual concerned;
- where necessary to avoid prejudice to the maintenance of the law;
- where necessary to avoid a serious threat to public health or safety or to the life or health of an individual; or
- made in a publicly available publication.

Sections 7 and 10(3) (or their replacements) should apply to the new measure.

R112 The Privacy Commissioner should have power to approve specified overseas privacy frameworks as providing acceptable privacy standards. The Office of the Privacy Commissioner should maintain a list of such frameworks on its website.

R113 The Privacy Commissioner should provide guidance for New Zealand agencies on conducting risk assessment prior to disclosing personal information overseas and on the use of contractual or other means to ensure the application of acceptable privacy standards.

R114 The Privacy Act should be amended to:

- enable the Privacy Commissioner to share relevant information with overseas privacy enforcement authorities relating to possible violations of privacy law;
- enable the Privacy Commissioner to provide assistance to overseas authorities relating to possible violations of the overseas country's privacy law;
- provide for requesting and giving mutual assistance between the Privacy Commissioner and his or her overseas counterparts;
- provide for cooperation with other authorities and stakeholders; and
- supplement the Tribunal's procedural powers to deal with cross-border privacy complaints.

R115 The Privacy Act should include a provision allowing for the future adoption of a cross-border privacy rules system in New Zealand. The provision should come into force at a time to be determined by Order in Council.

CHAPTER 12

R116 The Marketing Association's Do Not Call register should be put on a statutory footing under the reformed consumer legislation and the Ministry of Consumer Affairs should initiate the necessary policy work to progress this initiative.

R117 Principle 12 should be amended to encourage measures to control the public display of unique identifiers, as a response to the problem of identity crime. The following subclause should be added to principle 12:

(5) An agency that discloses or displays an individual's unique identifier must take such steps (if any) as are reasonable to minimise the risk of misuse of the unique identifier.

R118 The Privacy Commissioner should produce guidance for agencies on the range of options available to address the risk of misuse of unique identifiers, with reference to any relevant industry standards.

R119 Section 14 should be amended to provide that, in exercising his or her functions, the Privacy Commissioner must take account of Māori needs and cultural perspectives, and of the cultural diversity of New Zealand society.

R120 Principle 4 should be amended to provide that, in considering whether the collection of personal information is unfair or unreasonably intrusive for the purposes of principle 4(b), the age of the individual concerned must be taken into account. The Privacy Commissioner should develop guidance material with respect to this new provision.

R121 The Advertising Standards Authority, the Marketing Association and any other relevant industry bodies should review the adequacy of privacy protection in existing codes that regulate marketing to children.

R122 Section 14(b) should be amended to refer to New Zealand's international obligations concerning the rights and best interests of the child.

R123 The Office of the Privacy Commissioner should convene a working group to consider issues of capacity under the Privacy Act, and to develop guidance material based, as much as possible, on supported decision-making.

R124 Further work should be undertaken to explore issues of privacy and disability. This work should be facilitated by the Office of the Privacy Commissioner or another appropriate body, and should be carried out in partnership with disabled people's organisations.

R125 The Government should conduct a review of the handling of health information, with a view to enacting separate comprehensive legislation.

R126 Section 23 should be amended to allow agencies to appoint a privacy officer from outside the agency.

APPENDIX 2

These recommendations will only apply if the existing information matching regime is retained. (We have recommended that it be merged into the information sharing regime that we propose in appendix 1.)

R127 There should be a single definition of "information matching programme".

R128 The period of notice of adverse action provided for in section 103 should be 10 days, but with power in the Privacy Commissioner to reduce the period in appropriate cases.

R129 To the examples of "adverse action" in section 97 should be added decisions to impose a penalty and to recover a penalty or fine.

R130 Continuing programmes of information matching should have to be authorised, and operate, under Part 10 of the Privacy Act.

R131 Agencies seeking legislation to authorise an information matching programme should provide the Privacy Commissioner with a protocol describing the details of the programme; and the Privacy Commissioner should be able to require a Privacy Impact Assessment.

R132 There should no longer be a requirement of a five-yearly review by the Privacy Commissioner of every information matching provision, but the Commissioner should be able to conduct reviews as and when desirable.

R133 The government should be required to respond within six months of the presentation of a report on a review by the Privacy Commissioner of an information matching provision.

R134 The Privacy Commissioner should be able to report separately on information matching programmes rather than including such a report in his or her annual report.

R135 The information matching rules currently contained in Schedule 4 of the Privacy Act should be placed in the body of the Privacy Act, and the current rules 3 and 8 should be deleted.

R136 The current blanket exemptions for Inland Revenue contained in section 101(5) and rule 6(3) of schedule 4 should be repealed, but exemptions should be provided for in particular matching authorities where that is appropriate.

INFORMATION SHARING PROPOSALS IN APPENDIX 1

In our Ministerial Briefing of 29 March 2011, reproduced in this report as appendix 1, we put forward the following proposals on the issue of information sharing:

(1) That the Privacy Act 1993 should be amended to make provision for the approval of programmes for the sharing of personal information between government agencies.

(2) That such programmes should require approval by Order in Council.

(3) That the Privacy Act should expressly lay down the process of approval, which would involve consultation with appropriate persons including the Privacy Commissioner; the criteria for approval; the matters required to be contained in programme agreements; and general rules for the operation of such programmes. The general rules should provide safeguards, require transparency, and provide for means of accountability.

(4) That Orders in Council approving programmes should be disallowable instruments within the Regulations (Disallowance) Act 1989.

(5) That information matching should be treated as a form of information sharing, and be subject to the same processes and rules. Existing matching programmes should not have to be re-approved, but in their ongoing operation they should be subject to the new rules. The same should be true of law enforcement information currently contained in schedule 5 of the Privacy Act.

(6) That the proposed regime should apply to all continuing programmes of information sharing between government agencies. If, however, it is decided that approval should be required only for programmes which are not otherwise compliant with the Privacy Act, the transparency requirements should apply to the non-approved programmes.

(7) That, in the first instance, the proposed regime should apply only to sharing between central government agencies, although in appropriate cases it might be extended to include non-governmental organisations on the basis described in paragraphs [75] and [76] of the Ministerial briefing.

(8) That all approved programmes should be listed in a schedule to the Privacy Act 1993.

RECOMMENDATIONS FROM OTHER REPORTS

Some of our recommendations from stages 2 and 3 of the Review of Privacy are also relevant to this report.

Stage 2: Public Registers

Since public registers are currently regulated partly through Part 7 of the Privacy Act, the whole of our *Public Registers* report is also relevant to this stage 4 report. One of the recommendations in the *Public Registers* report (R7) was for specific amendments to the Privacy Act, as follows:

> We recommend that provision be made in the Privacy Act 1993 for applications for name and/or address suppression to the Privacy Commissioner, and that each public register statute should refer to the availability of such applications. The functions of the Privacy Commissioner in section 13 of the Privacy Act 1993 should include consideration of, and decisions upon, such applications.

Stage 3: Invasion of Privacy

There were two recommendations in our report for stage 3, *Invasion of Privacy: Penalties and Remedies*, which involved the Privacy Act. R18 and R19 were as follows:

> The Privacy Act should provide that one of the functions of the Privacy Commissioner is to report regularly to Parliament on developments in surveillance and surveillance technologies, and their implications for New Zealand.
>
> Both Closed-Circuit Television (CCTV) and Radio-Frequency Identification (RFID) should be regulated within the Privacy Act framework, rather than under specific statutes or regulations. The Privacy Commissioner should continue to monitor the adequacy of existing law to deal with these technologies. If a more specific regulatory framework is considered necessary in future, the option of developing codes of practice under the Privacy Act should be considered.

Chapter 1
Introduction

THE LAW COMMISSION'S REVIEW OF PRIVACY

1.1 This report marks the conclusion of the Law Commission's review of the law relating to privacy (the Review). The Review has been conducted in four stages, and this report completes stage 4. Stage 4 is a review of the Privacy Act 1993.

1.2 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 a study paper, which did not make any recommendations, in January 2008.[1]

1.3 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 are therefore not dealt with in the present report.

1.4 Stage 3 was concerned with the adequacy of New Zealand's civil, criminal, and regulatory law to deal with invasion of privacy, but did not focus 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.

1.5 This stage 4 report follows on from an issues paper published in March 2010.[4] We received around 80 submissions on the questions asked in the issues paper, from a range of public and private sector organisations and from a number of individuals. We have already reported on one aspect of our review of the Privacy Act. At the request of the Minister Responsible for the Law Commission, we prepared a Ministerial briefing on the issue of sharing of personal information between government agencies.[5] Our briefing on information sharing was released in March 2011, ahead of this report, because this issue was becoming a matter

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

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

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

4 Issues Paper (see Glossary for full citation).

5 Law Commission *Information Sharing: Ministerial Briefing* (2011).

of some urgency within government. Our policy advice to the Minister on information sharing is included in this report as appendix 1. Appendix 2 deals with the closely-related subject of information matching.

1.6 Now that the Review has been completed, the next step is for the Government to respond to the reports for stages 2, 3 and 4. The Government released a preliminary response to stage 3 of the Review in August 2010,[6] but deferred decisions on most recommendations until the completion of stage 4.

OTHER RELEVANT WORK

Privacy Commissioner statutory reviews of the Privacy Act

1.7 Section 26 of the Privacy 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 is to report his or her recommendations for amendments to the Act to the responsible Minister, who is to table the report in the House of Representatives. We discuss this provision further in chapter 5. The first of these periodic reviews resulted in a major report, entitled *Necessary and Desirable*, published in 1998.[7] Since then, four supplementary reports have been published by the Office of the Privacy Commissioner. In undertaking our own review of the Privacy Act, we have made extensive use of these reports, and many of our recommendations are based on the recommendations of the Privacy Commissioner's reviews. At the same time, we have not discussed in this report all of the issues raised in the Privacy Commissioner's reviews. It should not be assumed that we consider those recommendations of the Privacy Commissioner that are not taken up in this report to be without merit. Many of those recommendations concern points of detail or legal technicalities, and can be taken up in the drafting of a Bill to implement this report.

Work within government on privacy law reform

1.8 The Government has not yet implemented the recommendations of *Necessary and Desirable* and its supplements. When we commenced this review, work was under way within the Ministry of Justice on various operational and technical amendments to the Act, including amendments based on the recommendations of the Privacy Commissioner. In May 2008 the Government decided that it would be better to have a single stream of work considering reform of the Act, and that the work of the Privacy Commissioner and the Ministry of Justice should be taken into account as part of the Law Commission's review. The Government did, however, proceed with a Bill to address issues concerning cross-border transfers of personal information, in order to bring New Zealand's

6 *Government Response to Law Commission Report on Invasion of Privacy: Penalties and Remedies* (2010).

7 *Necessary and Desirable*, and *1st*, *2nd*, *3rd* and *4th Supplements to Necessary and Desirable* (see Glossary for full citations).

privacy law more closely into alignment with the European Union's directive on data protection. The Privacy (Cross-border Information) Amendment Act was passed in 2010, and is discussed further in chapter 11.

Australian reviews

1.9 Law reform agencies in Australia have been conducting their own reviews of privacy law in parallel to ours:

- The Australian Law Reform Commission (ALRC) has undertaken a major review of the Privacy Act 1988 (Cth), the Australian Federal information privacy law. The ALRC produced a comprehensive, three-volume report to the Australian Government in May 2008.[8]
- The New South Wales Law Reform Commission has reported on a statutory cause of action for invasion of privacy,[9] as well as on matters relating to information privacy statutes in New South Wales and their intersection with freedom of information legislation.[10]
- The Victorian Law Reform Commission has reported on two more specific issues: workplace privacy and surveillance in public places.[11]

All of these reviews are now complete. The Australian Government has released the first part of its response to the ALRC report, accepting many of its recommendations.[12] The Australian Government has also released exposure drafts of legislation to implement its response in relation to reform of the privacy principles and of credit reporting. These exposure drafts are currently being considered by the Senate Finance and Public Administration Committee.

1.10 We have found the reports of the Australian reviews very useful, and in stage 4 of our Review we have found it particularly helpful to refer to the ALRC report. We have taken account of the ALRC review partly because of its comprehensive consideration of the issues, and partly because of the desirability of achieving harmonisation between Australian and New Zealand privacy law where possible.

PRIVACY ACT 1993

1.11 The Privacy Act 1993 came into force on 1 July 1993. The legislative history of the Act is set out in some detail in our issues paper.[13] The Act deals mainly with informational privacy; that is, it regulates what can be done with information about individuals. It is not primarily concerned with spatial privacy, or control over access to our persons and to private spaces,[14] although (as we discuss further in chapter 5) the Privacy Commissioner does have some functions that extend beyond informational privacy. We briefly describe the Act here, and provide further detail in subsequent chapters.

8 *For Your Information* (see Glossary for full citation).

9 New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC R120, Sydney, 2009).

10 New South Wales Law Reform Commission *Privacy Principles* (NSWLRC R123, Sydney, 2009); *Access to Personal Information* (NSWLRC R126, Sydney, 2010); *Protecting Privacy in New South Wales* (NSWLRC R127, Sydney, 2010).

11 Victorian Law Reform Commission *Workplace Privacy: Final Report* (Melbourne, 2005); *Surveillance in Public Places: Final Report* (VLRC R18, Melbourne, 2010).

12 *Enhancing National Privacy Protection* (see Glossary for full citation).

13 Issues Paper at 17–24.

14 On the distinction between informational and spatial privacy, see Law Commission *Privacy: Concepts and Issues,* above n 1, at 57–60.

1.12 The coverage of the Act is quite broad. It applies to "personal information", or information about identifiable, living individuals, and is not limited to information that is considered particularly sensitive or private.[15] Personal information must be handled in accordance with 12 information privacy principles that are set out in the Act.[16] These principles are concerned with how personal information may be collected, held, used and disclosed. Any "agency" must comply with these principles, and an agency can be any person or body in either the public or the private sector. However, certain entities (such as the news media) are excluded from the definition of "agency". The Act also contains various other exclusions and exemptions from the coverage of the privacy principles, and a number of the principles themselves contain exceptions.[17]

1.13 The Act establishes the office of a Privacy Commissioner.[18] The Commissioner is an independent Crown entity,[19] which means that the Commissioner is generally independent of Government policy. Sir Bruce Slane was the first Commissioner, and he was replaced by the current Commissioner, Marie Shroff, in 2003. The Commissioner's functions include investigating complaints of breaches of the Act; advising government on privacy issues; and providing general education and advice on matters relating to privacy protection.[20] Complaints under the Act are made initially to the Privacy Commissioner.[21] The Commissioner investigates complaints and, if they appear to have substance, attempts to secure a settlement between the parties. If no settlement can be reached, the complaint can proceed to the Human Rights Review Tribunal, which is able to grant remedies if it finds that there has been an interference with the complainant's privacy.

1.14 The Act also contains provisions dealing with certain specific matters:

- Part 6 of the Act authorises the Privacy Commissioner to issue codes of practice.[22] Such codes can deal with particular types of information, agency, activity or industry. They can modify the application of the privacy principles by prescribing standards that are more or less stringent than those in the principles, or by exempting actions from the principles. A number of codes are currently in force, covering areas such as health and credit reporting.
- Part 7 and schedule 2 of the Act deal with public registers. Part 7 sets out four privacy principles that apply specifically to public registers. As noted above, public registers were the subject of stage 2 of this Review, so they will not be covered in this report.

15 The definition of "personal information" is discussed further in ch 2.

16 See ch 3. The privacy principles are set out in full in appendix 3 of this report.

17 On exclusions and exemptions from the Act, see ch 4. Exceptions to the principles are discussed in ch 3.

18 Privacy Act 1993, s 12.

19 Crown Entities Act 2004, sch 1, part 3.

20 On the Commissioner's functions, see ch 5.

21 Complaints and enforcement are discussed further in ch 6.

22 See ch 5.

- Part 10 and schedules 3 and 4 of the Act impose controls on information matching by public sector agencies.[23] Information matching involves the comparison of personal information from different sources in order to produce or verify information about an individual.
- Part 11 and schedule 5 of the Act are concerned with the sharing of personal information between public sector agencies for law enforcement purposes.[24]
- Part 11A of the Act imposes some controls on the transfer outside New Zealand of personal information.[25]

OUR APPROACH IN THIS REVIEW

1.15 In reviewing the Privacy Act, we have kept 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.

23 See appendix 2, and Issues Paper at ch 9.

24 See ch 9.

25 See ch 11.

Chapter 2

Scope, approach and key definitions

2.1 The Privacy Act is notable for its broad coverage and its flexible, principles-based approach. In the issues paper we asked about the appropriateness of the current scope and approach of the Act, including whether it strikes the right balance between privacy and other competing interests.[26] We also asked whether any changes could be made to help ensure that public perceptions of the Act better match its actual objectives and application. We discuss these issues in this chapter. Central to the scope of the Act are the definitions of certain key terms, and we discuss those terms in this chapter as well. Specifically, we discuss the meaning of "personal information", "individual", "collect" and "publicly available publication".

2.2 Overall, the scope of the Act is very wide in that it applies to almost all agencies, whether in the public or the private sectors, and to all "personal information" (which is defined broadly). The focus of the Act is on privacy of personal information, although, as we discuss in chapter 5, the Privacy Commissioner also has some functions that relate to privacy in a broader sense. There are some exclusions and exemptions from the Act's coverage, which we discuss in chapter 4. As we discuss in this chapter, the Act applies only to information about natural persons (not corporations or groups) and, for the most part, it does not apply to information about deceased persons.

2.3 We consider that the Act's broad scope and coverage is appropriate because it ensures that protection of informational privacy is as comprehensive as possible. In some other jurisdictions a patchwork of subject-specific privacy laws, or different laws for the public and private sectors, create uncertainty and gaps in coverage. By contrast, we believe that New Zealand is well served by having a single, comprehensive information privacy law. The corollary to this belief is that the Act must be flexible enough to apply in a wide range of circumstances. Our views on the approach that the Act should take to the protection of informational privacy are in line with this conclusion.

26 Issues Paper at ch 2.

A NEW ACT

2.4 We do not think that the approach of the Privacy Act is fundamentally flawed or that root-and-branch reform of the Act is needed. On the contrary, we think that the Act generally works well.

2.5 At the same time, we make many recommendations for changes to the Act in the course of this report. Some of these changes are quite far-reaching; many others concern points of detail, although their implications may still be quite significant. In addition, as we mention below, there are other technical and structural changes that could usefully be made to the Act, but that are not discussed in this report. Because we propose to make so many changes to the Act, we believe that the current Act should be repealed and replaced by a new Act. Amendment Bills that introduce numerous changes to existing statutes are a recipe for messy and inaccessible legislation. In recent years, the Legislation Advisory Committee (a body that advises the government on good law-making practice) has indicated a strong preference for new statutes rather than amending legislation where the changes to an existing statute are extensive.

2.6 The drafting of a new Act will also be an opportunity to deal with a range of structural and technical issues that are not discussed in this report. In our issues paper we asked whether the Privacy Act could be better structured to make it easier to navigate and read. We got a number of suggestions for restructuring in submissions, and these can be taken into account in the drafting of a new Act. Drafting of a new Act should also take into account the recommendations for restructuring the Act, and generally making it clearer and easier to navigate, that have been made by the Privacy Commissioner in *Necessary and Desirable* and its supplements. In addition, the Privacy Commissioner has made various recommendations for technical amendments to the Act that we do not discuss in this report, but that are nonetheless worthwhile. We would expect the Office of the Privacy Commissioner (OPC) to be a key player in the drafting of a new Act, and thus to be in a position to ensure that such changes are not overlooked.

2.7 We also asked in the issues paper whether the names of the Privacy Act and the Privacy Commissioner should be changed, mainly to highlight the focus of the Act on informational privacy rather than other aspects of privacy. Although some submitters favoured a change, most did not. Submitters who opposed the change argued that the current names are well-established, and that changing them would create confusion and uncertainty. We agree. Moreover, we recommend in chapter 5 that the Privacy Commissioner's statutory functions should continue to extend more widely than informational privacy in some respects. The names "Privacy Act" and "Privacy Commissioner" are not misleading, and are well-known and understood. They should be retained.

2.8 Although we recommend the enactment of a new Act, as a matter of convenience we will refer in this report to amending particular sections of the current Act where appropriate.

RECOMMENDATION

R1 A new Privacy Act should be enacted. In addition to implementing the recommendations of this report, it should incorporate changes recommended by the Privacy Commissioner in *Necessary and Desirable* and its supplements.

THE PRINCIPLES-BASED APPROACH OF THE ACT

2.9 The Act deliberately takes a flexible, open-textured approach to regulating the collection, storage, use and disclosure of personal information. Rather than setting out strict rules about how personal information may be handled, the Act is based on a set of 12 privacy principles. These principles provide agencies with a high degree of flexibility in terms of how they comply with them.

2.10 In our issues paper, we considered the arguments for and against a principles-based approach to information privacy regulation.[27] Our preliminary conclusion was that the Act should continue to take a principles-based approach. This was not only because we wanted to retain the Act's flexibility, but also because we wanted to ensure that it is "future-proofed". An open-textured Act is less likely to be overtaken by developments in technology than one that sets out strict rules.

2.11 There was overwhelming support in submissions for retaining the Act's principles-based approach; indeed, there were no submitters who favoured moving towards a more prescriptive, rules-based approach. Arguments put forward in submissions in favour of the principles-based approach were that it is:

- flexible and adaptable – agencies can apply it in the way that best fits their circumstances;
- outcomes-focused;
- able to respond to technological and social change;
- effective in encouraging good behaviour; and
- consistent with the approach in information privacy statutes in other jurisdictions, and in transnational privacy instruments.

2.12 We agree with these arguments, and our view that the Act should continue to be open-textured and principles-based is unchanged. As submitters noted, the Act provides more specificity where it is needed. For example, the provisions of the Act dealing with access and correction are more prescriptive, and codes of practice can also provide greater specificity as to how the principles apply to particular sectors. We believe the Act currently gets the balance between flexibility and specificity right.

2.13 A consequence of retaining the flexibility that is inherent in the principles-based approach is that the Act does not provide the certainty of "bright line" rules. We acknowledge that this creates some compliance costs, as each agency must take the time, or pay for legal advice, to assess how the principles apply to its activities. However, we believe that the inflexibility of a rules-based system would create greater compliance costs. A privacy law practitioner who also provides seminars on privacy law on behalf of OPC commented in a submission that the principles-based approach is not as difficult as it may appear. If agencies identify the purposes for which they collect information clearly, compliance with the other principles becomes more straightforward. She also observed that the overwhelming response of participants in Privacy Act seminars is that compliance with the Act is straightforward and that all they need to do is to develop a policy and incorporate it into the culture of the agency.

27 Ibid, at 28–32.

2.14 However, we do understand that the absence of "bright line" rules can create a degree of uncertainty about the application of the Act, and can lead to misunderstandings about what the Act requires (as we discuss further under "Perceptions of the Act" below). The open-textured nature of the Act can create difficulties for frontline staff who have to apply it in their interactions with the public. Such staff may have only a minimal understanding of the privacy principles, and yet may face challenging situations in which privacy must be balanced with other interests. We are sympathetic to the difficulties that agencies sometimes face in applying the Act, but once again we think that greater difficulties would be created by making the Act more prescriptive. It would not be possible in a rules-based system to take proper account of the many different contexts in which agencies operate, and to provide agencies with the flexibility they need to carry out their business effectively. We think that the answer to uncertainty about the Act's application must lie with training and guidance within agencies, as well as with public education about the Act.

RECOMMENDATION

R2 The Privacy Act should continue to take an open-textured, principles-based approach to regulating information privacy.

PRIVACY AND OTHER INTERESTS

2.15 Privacy is not an absolute right or value; it can justifiably be overridden in particular circumstances by other rights and interests.[28] The Privacy Act recognises this fact in a number of ways. The Act includes a range of exceptions in the principles themselves (discussed in chapter 3), as well as other exemptions and exclusions (discussed in chapter 4), which recognise interests that can override the protection of privacy. For example, there are exceptions relating to the maintenance of the law, which recognise the importance of detecting and prosecuting offences. Section 14(a) of the Act also recognises that privacy cannot be considered in isolation from other interests. It requires the Privacy Commissioner, in the performance of his or her functions, to have due regard to the protection of important 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".

2.16 In general, submitters on the issues paper thought that the Privacy Act gets the balance between privacy and other interests about right. A few government agencies thought that the Act itself, or the enforcement of the Act, does not always give sufficient recognition to other competing interests. Some suggested that the issue of balancing privacy and other interests could be addressed in a new purpose clause for the Act, which is a matter we discuss further below. The Children's Commissioner said that recognising the "best interests of the child" principle in the Act would help to ensure that the right balance is struck in matters involving children, and we consider this proposal in chapter 12.

28 We discussed the balancing of privacy and other interests in Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008) at 185–191.

2.17 The strongest suggestion that the Act does not get the balance right at present came in the submission from the Police, who considered that the wrong balance is struck in the law enforcement area. To illustrate this view, the Police raised a number of specific issues, including perceived abuse of access rights under the Act and the way in which, in the Police's view, the Act inhibits agencies from disclosing personal information that might be of assistance to the Police. We deal with some of these issues later in this report.

2.18 OPC, by contrast, submitted that the Act does not provide sufficiently strong privacy protection and may need rebalancing, particularly in light of technological developments since 1993. OPC saw strengthening of enforcement powers as the most important change needed to provide a proper balance. In this report we recommend that the Privacy Commissioner be given some new powers, which we believe will increase the Act's effectiveness.

2.19 The issues paper also asked about compliance costs imposed by the Act, an issue which involves striking an appropriate balance between providing effective privacy protection and allowing both business and government to operate efficiently.[29] We consider that the Act takes a light-handed approach to regulation, and unlike in some other jurisdictions, agencies are not required to register with or pay fees to the Privacy Commissioner. The Act's flexibility and the emphasis of the complaints process on conciliation rather than on the imposition of penalties help to minimise compliance costs. This view is borne out by research on compliance costs under the Act.[30] Nonetheless, we were interested to hear whether there are ways in which compliance could be made easier and less costly without compromising the Act's objectives.

2.20 Some agencies said that they do not find compliance to be a burden, or that they accept the costs as a necessary part of carrying out their work. OPC commented that compliance costs imposed by the Act are modest and are outweighed by the benefits of good information practice. OPC also noted that it assists agencies with compliance with the Act, and suggested that modest additional resourcing could help it to provide an increased level of guidance and assistance without compromising its other responsibilities. The usefulness of guidance from OPC in reducing compliance costs was endorsed by other submitters.

2.21 One submission said that compliance with the Act is a particular burden for not-for-profit agencies, which are often staffed by volunteers, and that such agencies should receive funding support to deal with privacy issues. Another submitter said that the cost of attending OPC's workshops on Privacy Act compliance was an obstacle to participation, and that such workshops should be free. In general, however, submitters did not indicate that compliance with the Privacy Act is currently a major burden for agencies. At the same time, there was a significant level of concern expressed about the potential for reforms to the Act discussed in the issues paper to upset the existing balance and to introduce substantial new compliance costs. We have been mindful of such concerns in framing our recommendations in this report.

29 Issues Paper at 35–38.

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

2.22 Overall, we believe that the Privacy Act strikes the right balance between privacy and other interests, and does not impose unreasonable compliance costs. Some of our recommendations involve a degree of rebalancing in particular areas, but we do not see any need for sweeping changes. We also recommend below that a new purpose clause for the Act should reflect the fact that other interests will sometimes override the protection of personal privacy.

PERCEPTIONS OF THE ACT

2.23 We asked in the issues paper about people's perceptions of how the Act is operating in practice, and whether any perceived deficiencies are due to the Act itself or to the way in which it is understood and applied.[31] We did so, in part, because the Privacy Act is sometimes blamed for unreasonably preventing the release of personal information. Such blame is often not justified; indeed, the acronym BOTPA (Because of the Privacy Act) has been coined to describe situations in which an agency uses the Privacy Act as a reason for failing to release information when in fact the failure to disclose has nothing to do with the Act. Often such cases are due to a lack of understanding of the Act, but sometimes an agency may shelter behind the Act when it does not wish to release information for other reasons. Sometimes, too, an agency may refer to "the Privacy Act" when in fact what is meant is something else altogether, such as professional confidentiality. Conversely, a vague reference by the agency to "privacy reasons" may be interpreted by a person requesting information or by the news media as being a reference to the Privacy Act. Nonetheless, perceptions can be powerful, and we asked submitters to consider whether changes to the Act could help to ensure that public perception and understanding of it more correctly match its objectives.

2.24 In general, submitters considered that the Act is working well and that problems commonly stem from misunderstandings of the Act. They said that education and guidance about the Act (both within agencies and among the general public) can help to deal with such misunderstandings, while some submitters also considered that a new purpose clause for the Act could help. A few submitters suggested that negative media coverage had fuelled misconceptions about the Act. OPC cautioned that changing the law will not be an effective strategy for addressing problems of perception if those perceptions are not based on what the law actually says. OPC sees privacy officers as having a key role to play in ensuring that agencies implement the Act effectively and sensibly.

2.25 On the whole, we agree with OPC and others that the problems of misunderstanding or misperception of the Act cannot be solved by changing the Act itself. We endorse the importance of providing training and guidance on the Act within agencies, and of educating the public about the Act. Such strategies are the most effective ways of ensuring that implementation and perceptions of the Act match its objectives. However, some of our recommendations for reform of the Act, while not designed to address perception problems, may nonetheless deal with areas in which such problems exist. In particular, negative coverage of the Act sometimes focuses on a failure to share personal information between government departments for socially-beneficial purposes. Our proposals for a new information sharing framework, discussed in appendix 1, should allow government agencies to share personal information as part of properly-authorised programmes, while still maintaining appropriate privacy safeguards.

31 Issues Paper at 41–43.

GUIDANCE

2.26 A number of the issues discussed above – uncertainty about the application of the privacy principles, striking the right balance between privacy and other interests, reducing compliance costs, and improving understanding of the Act – could be addressed partly by means of guidance material about the Act. In many cases OPC is the most obvious body to provide such guidance, but guidance can also be provided (in consultation with the Privacy Commissioner) by other agencies which possess specialised knowledge in a particular area, or which represent a particular industry or sector.

2.27 OPC already produces a variety of different types of guidance, including:

- information on the OPC website;[32]
- brochures about privacy rights and obligations;[33]
- booklets about compliance with the Act in particular areas, such as schools and workplaces;[34] and
- more formal guidelines about issues such as responding to data security breaches, and privacy and closed-circuit television (CCTV).[35]

In the issues paper, we asked about the usefulness of such guidance, particularly from the Privacy Commissioner.

2.28 Submitters generally said that they find Privacy Commissioner guidance useful. It was suggested that guidance which provides specific examples is particularly helpful. However, some notes of caution were struck. The internet search company Google said that guidance material should only be produced after consultation with affected stakeholders. The then chair of the Human Rights Review Tribunal, Royden Hindle, said that Privacy Commissioner guidance is very useful, but it should not be seen as having anything like legislative effect, or as deriving from a sort of delegated legislative power. He considered that a reasonably intelligent lay reader of the Act should be able to understand what the Act says without having to resort to guidance material. The importance of clearly distinguishing guidance from law was also emphasised by some other submitters. OPC itself noted that developing guidelines can be resource-intensive, and that there is a limit to how much guidance can realistically be produced compared to how much might be desirable. OPC also noted that there can be a useful role for industry or sectoral bodies, rather than the Privacy Commissioner, in developing guidance. While OPC possesses expertise in the interpretation of the privacy principles, sectoral bodies may possess greater understanding of how personal information is used in a particular sector, and may be more successful at achieving "buy in" to the guidelines within the sector in question.

32 See Office of the Privacy Commissioner "How to Comply" < http://privacy.org.nz/how-to-comply-with-the-privacy-act > .

33 See, for example, Office of the Privacy Commissioner *Good Privacy is Good Business* and *Health Information Check-up.*

34 Office of the Privacy Commissioner *Privacy at Work: A Guide to the Privacy Act for Employers and Employees* (Wellington, 2008); 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).

35 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, 2008) and *Privacy and CCTV: A Guide to the Privacy Act for Businesses, Agencies and Organisations* (Wellington, 2009).

2.29 We have been conscious in this report of the cautionary points raised in submissions with regard to guidance from the Privacy Commissioner. We are aware of the resource constraints on OPC, and have tried to limit the number of areas in which we recommend that OPC should develop guidance material. Where we have recommended the development of guidance, we leave it to OPC to consider what form such guidance should take. In many cases detailed guidelines will not be required, and it may be sufficient to put a discussion of the particular issue on the OPC website, for example. We also agree with the submitters who were concerned that guidance should be clearly distinguished from law. Unlike codes of practice (discussed in chapter 5), guidelines and similar documents are *not* a form of delegated legislation but simply a guide to good practice in complying with the Act. It is important that they are not seen as imposing rigid rules, or as taking the place of the Act itself. So long as its nature and effect is clearly explained, as it is in documents produced by the Privacy Commissioner, guidance material is very useful in assisting people to comply with and exercise their rights under the Privacy Act, and production of such material is to be encouraged.

2.30 There could, however, be one issue. If an agency relies on an interpretation tendered in guidance material, would that reliance be a defence if there were a complaint about the agency's behaviour? One would have thought that the Privacy Commissioner, even though not legally bound by the guidance, would in practice follow it. A question of estoppel might even arise. It would be different, however, if the matter were to proceed to the Human Rights Review Tribunal. Should the Tribunal not agree with the guidance, it would be free to depart from it, although presumably the Tribunal would take the guidance into account in deciding on the appropriate redress. We have decided to make no recommendation about this, but urge the Privacy Commissioner, and others issuing guidance, to take care to distinguish guidance from lawmaking, and therefore to beware of giving any impression that guidance can place an authoritative interpretation on a statutory term which is genuinely ambiguous.

A PURPOSE PROVISION FOR THE ACT

2.31 The Privacy Act currently has a long title, which 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.

To comply with modern drafting style, the long title should be replaced by a purpose section, the aim of which is to assist with the understanding of the Act. The purpose section could simply repeat the wording of the long title almost

word for word. However, the drafting of a purpose section for a new Privacy Act is an opportunity to consider whether the current wording remains a useful statement of the Act's purpose.

2.32 In the issues paper we asked whether the Privacy Act should contain a purpose section and, if so, what its content should be. There was significant support from submitters for the inclusion of a purpose section in the Act. Some submitters thought that a new purpose provision should simply be based on the current long title. However, a number of submitters said that the purpose clause should specifically refer to balancing privacy with other rights and interests, an issue which we discuss below. OPC said that a purpose provision could "emphasise the Act's wider aims of empowering individuals to maintain control over their personal information." OPC also cautioned that:

> a purpose clause may unintentionally create new difficulties in operating the legislation. In particular, it would be problematic if the clause were to create new opportunities for argumentative parties to complaints.

We are aware of this danger, but believe that, with careful drafting, such difficulties can be avoided and a purpose provision for the new Privacy Act can instead aid interpretation and understanding.

2.33 The most difficult issue we have had to consider in relation to a purpose section for the Act is how, if at all, the provision should deal with the relationship between privacy and other interests. We have already referred above to section 14(a) of the Act, which requires the Privacy Commissioner, in exercising his or her powers under the Act, to have regard to other rights and interests that compete with privacy. This section, however, applies only to the Commissioner, whereas a purpose section would also assist agencies and individuals in interpreting and applying the Act. The Australian Law Reform Commission has recommended that there should be a new objects clause in the Privacy Act 1988 (Cth), and that one of the objects of the Act should be to:[36]

> recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance the public interest in protecting the privacy of individuals with other public interests.

In our issues paper, we suggested that the inclusion of a similar clause in a purpose provision for the New Zealand Privacy Act "might operate as a useful disincentive to treating privacy as the be-all and end-all, indicating that it is indeed subject to exceptions."[37] This suggestion was supported by a number of submitters.

2.34 We think that the Privacy Act's purpose section should recognise that privacy is not an absolute right which always "trumps" other rights and interests. We considered doing this by referring in the purpose provision to "balancing" privacy and other rights and interests. However, while the concept of "balancing" is one with which the courts are very familiar (including in privacy cases), its meaning may not be entirely clear to ordinary users of the Act. Moreover, it might be thought that a reference to balancing is intended to describe a process

36 *For Your Information* at recommendation 5–4.

37 Issues Paper at 40.

that is additional to the requirements of the operative provisions of the Act. It is not our intention to add a new step or a new consideration to decision-making about the handling of personal information. We therefore think it would be better for the purpose provision to refer to the fact that the scheme of the Act itself recognises, through exceptions to the principles and exemptions from the Act, that in some circumstances other interests will legitimately override privacy.

2.35 Another issue is whether the purpose provision should refer generally to international privacy standards, and whether it should refer specifically (as the long title currently does) to the OECD Guidelines. We think the purpose section should refer to international privacy standards and obligations. The origins of the Privacy Act lie partly with New Zealand's obligations under international human rights law, and with international privacy standards, particularly the OECD Guidelines. This fact should be reflected in the purpose provision. It is also important that the Privacy Act should remain consistent with international privacy standards as those standards continue to evolve. In this respect, we note that the APEC Privacy Framework has come into existence since the Privacy Act was passed, and that the OECD Guidelines are to be reviewed in 2011. There is also the possibility of an international privacy treaty or convention at some time in the future. New Zealand law must keep up to date with these developments, in order to remain broadly consistent with the laws of our trading partners. It is not strictly necessary for the purpose section to continue to refer to the OECD Guidelines, and one submitter said that the reference to the Guidelines in the long title opens up interpretation issues. However, OPC advises us that the purpose provision should continue to refer to the Guidelines, and we are inclined to accept their advice on this matter. The Guidelines remain probably the most widely-accepted international standard for information privacy protection. The principles from the OECD Guidelines are now expressly referred to in Part 11A of the Act and set out in Schedule 5A, both of which were inserted by the Privacy (Cross-border Information) Amendment Act 2010.

2.36 We recommend that the Privacy Act should have a purpose section. The purpose section should state that the purposes of the Act are to:

- promote and protect privacy of personal information, subject to exceptions and exemptions which recognise other rights and interests that will sometimes override privacy;
- provide for access by individuals to their personal information that is held by agencies, and for correction of such information;
- provide remedies for interferences with privacy of personal information;
- give effect to internationally-recognised privacy obligations and standards, including the OECD Guidelines; and
- make other provision for the protection of individual privacy.

RECOMMENDATION

R3 The Privacy Act should have a purpose section, which should state that the purposes of the Act are to:

- promote and protect privacy of personal information, subject to exceptions and exemptions which recognise other rights and interests that will sometimes override privacy;
- provide for access by individuals to their personal information that is held by agencies, and for correction of such information;
- provide remedies for interferences with privacy of personal information;
- give effect to internationally-recognised privacy obligations and standards, including the OECD Guidelines; and
- make other provision for the protection of individual privacy.

DEFINITIONS

2.37 Section 2 of the Privacy Act defines various terms used in the Act. One of these terms is "agency", which is defined very broadly: "any person or body of persons, whether corporate or unincorporated, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a Department". However, "agency" is also defined as excluding certain entities or types of entity that are listed in the definition; we discuss these exclusions from the definition of "agency" in chapter 4. We also discuss certain other definitional issues elsewhere in this report. In this chapter we examine a few key terms whose definitions are central to the scope and coverage of the Act. These terms are "personal information", "individual", "collect" and "publicly available information".

"Personal information"

2.38 The definition of "personal information" is central to the scope of the Act as a whole, since all of the privacy principles apply only to information that is "personal information".[38] "Personal information" is defined as:

> information about an identifiable individual; and 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.

This definition is very broad, and is not limited to information that is particularly sensitive, intimate or private. The Privacy Act, unlike some similar statutes in other jurisdictions, does not have a separate category of "sensitive information": all personal information is treated in the same way under the Act.

2.39 Leaving aside the part of the definition that deals with information relating to a death (which we discuss below in relation to "individual"), the definition of "personal information" has four elements: "information"; "about"; "identifiable"; and "individual". "Individual" is defined separately, and is discussed later in this

38 For further discussion of "personal information" under the Privacy Act see ibid, at 45–60; Paul Roth "What is Personal Information?" (2002) 20 NZULR 40 ["What is Personal Information?"]; Katrine Evans, Assistant Commissioner (Legal and Policy), 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).

chapter. In the issues paper, we asked whether any of these elements needed clarification and, if so, how this should be done. We said that there are three ways in which areas of uncertainty in relation to the definition of "personal information" could be dealt with:

- the definition in the Act could be amended;
- the Privacy Commissioner could provide guidance on the definition; or
- Privacy Commissioner case notes, and decisions of the Tribunal and the courts in particular cases, could help to resolve areas of uncertainty.

We also emphasised that, while determining what is or is not personal information can be very difficult in some circumstances, the areas of uncertainty arise only at the margins. In most cases, it will be quite clear whether information is "personal information" or not.

2.40 Overall, we got a fairly mixed response to our question about clarification of the definition of "personal information". Some submitters discussed issues relating to the definition, but did not necessarily anticipate that difficulties of interpretation could be solved either by amending the definition or by providing guidance. A number of submitters stated clearly that the current definition should not be changed, either because it presents no significant problems or because any attempt to provide greater clarity is unlikely to be successful. We discuss each element of the definition, and issues raised about those elements in submissions, below.

"Information"

2.41 "Information" is not defined in either the Privacy Act or the Official Information Act, but it seems clear that it can include information collected or held in a variety of forms, including audio and visual recordings.[39] It is also clear from decisions in cases under the Privacy Act and official information legislation that unrecorded matter held in an individual's mind can be information. This is in contrast to most overseas privacy statutes, whose coverage is limited to information that is recorded in some form. It seems reasonably clear, too, that information includes opinions and false information. If false information were not included in the meaning of "personal information", the right to seek correction of personal information in privacy principle 7 would be nonsensical. Likewise, if "personal information" did not include opinions, there would be no need to provide in section 29 that agencies can refuse requests for access to certain types of "evaluative or opinion material" (such as employment references).[40]

2.42 Submitters were generally comfortable with the "information" element of the definition. A number said that the definition should continue to include information that is held only in a person's mind and is not recorded in a document. We agree that unrecorded information should continue to be covered by the Act, and believe that to do otherwise would leave a significant gap in the

39 The scope of "information" under the Privacy Act is discussed in more detail in Issues Paper at 46–49. The *Oxford English Dictionary* has recently revised its definition of "information", which now runs to 9,400 words: James Gleick "The Very Word" (9 December 2010) Bits in the Ether < http://around.com > . See further James Gleick *The Information: A History, a Theory, a Flood* (Fourth Estate, 2011).

40 Section 29(1)(b) provides that access can be refused to "evaluative material" supplied in confidence. Section 29(3) defines "evaluative material" as meaning certain types of "evaluative or opinion material".

protection of informational privacy. Disclosure of unrecorded information in breach of principle 11, or use of unrecorded information whose accuracy has not been checked (in breach of principle 8), can be just as harmful to an individual as equivalent actions involving information in a document. Individuals should also have the right to obtain access under principle 6 to information about themselves that has not been written down or otherwise recorded. Such information can influence an agency's dealings with an individual just as much as documented information. Moreover, if it were not covered by the Act, agencies might have an incentive not to keep records concerning an individual or to destroy such records in order to frustrate the individual's access rights. A few submitters said that information held in a person's mind should only be covered by the Privacy Act if it is used in some way. We do not think that an amendment along these lines would be helpful, as there are other features of the Act that help to keep the Act's application to unrecorded information within reasonable limits. In particular, a number of privacy principles require agencies to take only such action as is reasonable in the circumstances, and agencies are only responsible for information held by employees in their capacity as employees (as opposed to their private capacities).[41]

2.43 Although the meaning of "information" is probably the least problematic element of the definition of "personal information", the definition could be amended to put certain matters beyond doubt, as the equivalent definition in the Privacy Act 1988 (Cth) does.[42] The definition could make clear that "personal information" includes:

- opinions;
- false information; and
- information that is not recorded in a document.

Such an amendment might make matters clearer to those who are not familiar with the Act, and could help to prevent current understandings being overturned by a future court decision. There was little call in submissions for the definition of "personal information" to expressly include opinions, false information and information that is not contained in a document. While there is some merit in making it clear that such information is included in the definition, there is also merit in keeping the definition succinct. On balance, we do not think that the "information" element of the definition needs further clarification.

"About"

2.44 Deciding whether or not information is "about" an identifiable individual can be the most difficult part of determining whether information is "personal information" or not.[43] A decision of the English Court of Appeal has taken a narrow view of what constitutes information "about" an individual for the purposes of the definition of "personal data" under the Data Protection Act 1998 (UK). The decision indicated that it should be information that is "biographical

41 Privacy Act 1993, s 3 deals with when information is considered to be held by an agency; see also ss 4, 126.

42 See definition of "personal information", Privacy Act 1988 (Cth), s 6. The ALRC has recommended leaving unchanged those elements of the definition that deal with false information, opinions, and information that is not recorded in a material form: *For Your Information* at 306, 309 (recommendation 6–1).

43 This issue is discussed in more detail in Issues Paper at 49–51.

in a significant sense" or that has the individual as its focus, rather than simply recording a matter or event in which the individual was involved or had an interest.[44] The majority of the New Zealand Court of Appeal, in obiter comments in *Harder v Proceedings Commissioner*, seemed similarly inclined to read down the meaning of "personal information" by limiting it to information that is "about" an individual in a fairly narrow sense.[45] However, there has been no authoritative decision on this point so far in New Zealand. In general, the Privacy Commissioner, the Tribunal and the courts have not taken a narrow view of when information is "about" an identifiable individual.

2.45 In the issues paper we gave a number of examples of situations in which it can be difficult to decide whether information is "about" an individual or not.[46] We also commented that it is unlikely that amending the definition of "personal information" could provide greater clarity in such cases, a point with which several submitters agreed. A submission from a law firm proposed that the Act should provide that information is not "about" an individual purely by virtue of that individual being named or referred to in correspondence. We do not think that such an amendment would provide greater clarity, and we think it might in fact create further confusion. In our view, the "about" element of the definition of "personal information" cannot readily be clarified by amending the definition or even by means of guidance because it is inevitably a matter that depends on the facts of the specific case.

"Identifiable"

2.46 The definition of "personal information" does not require that the individual be "identified" in the information, but rather that he or she must be "identifiable". The Privacy Commissioner, the Ombudsmen and the courts have taken the view that an individual can be identifiable if he or she can be identified from the information in question in combination with other information; that is, an individual does not have to be identifiable from the internal evidence of the information in question alone.[47] Even if this view is accepted, however, at least two areas of uncertainty remain:

- By whom must the individual be identifiable? Must the individual be identifiable to casual observers, or is it enough that the individual can be identified by those who know him or her well? What if the individual can only be identified by himself or herself?
- What if it is possible in theory to identify an individual, but such identification would require considerable time, expense or commitment of resources? Is it enough that identification is theoretically possible, or must it be reasonably practicable?

2.47 On the first of these points, a Tribunal decision indicates that an individual does not have to be identifiable to the world at large; it is enough that those who know the individual can identify him or her from the information in question.[48]

---

44 *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at [28].

45 *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 (CA) at [23]–[24].

46 Issues Paper at 51.

47 Roth "What is Personal Information?", above n 38, at 48–50.

48 *Proceedings Commissioner v Commissioner of Police* Complaints Review Tribunal 37/99, 16 December 1999.

On the second point, we gave examples in the issues paper of legislation, guidance and other instruments from overseas that attempt to provide greater clarity and assistance with regard to the feasibility of identification.[49] We also noted that advances in technology have made it easier to reidentify information that has been anonymised or deidentified, and that this may have implications for the concept of "identifiability" in future.[50]

2.48 The question of identifiability provoked more comments in submissions than did the other elements of the definition of "personal information". A number of submitters said that it would be useful to clarify what "identifiable" means, particularly with reference to:

- information that does not identify an individual on its own but can identify an individual when combined with other information; and
- the means and practicability of identification.

A number of submitters thought that, for information to be "personal information", it must be more than simply theoretically possible to identify an individual: it must be reasonably practicable to identify him or her. Google submitted that:

> where an individual is not identified, what could theoretically be done to enable an individual to become identifiable should not be treated in isolation from whether the provider is reasonably likely to combine the information and/or has undertaken not to do so in determining whether information is personal information.

Google pointed out that in some cases it would be unlawful or in breach of contract for an agency to combine sets of non-identified data, and suggested that in such cases the information in question should not be considered "personal information", even though it is theoretically possible that individuals could be identified by combining the data sets. In Google's submission, an unduly expansive definition of "personal information" would, if applied to internet services, subject service providers to:

> potentially unnecessary regulation as to collection, notification and use of disaggregated and uncombined pieces of information that are integral to provision of services, but are not intended to be brought together to identify a particular individual.

2.49 OPC acknowledged the increasing ease with which information that at first appears to be unidentifiable can be used to identify an individual, given technological advances that have made it easier to locate and combine information. They considered that the focus of the definition of "personal information" on information about identifiable individuals was still valid, but said that over time more information will start falling within the definition. They also noted that several of the privacy principles, as well as section 22H of the Health Act 1956, provide exceptions where personal information is anonymised or deidentified.

49 Issues Paper at 53–54.

50 See Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1701. For a contrasting view, see Jane Yakowitz "Tragedy of the Data Commons" (2011) Social Science Research Network < www.ssrn.com > .

2.50 Two academics specialising in privacy law raised issues about information that relates to more than one person. Gehan Gunasekara from Auckland University drew attention to the aggregation of personal information in such a way that it no longer relates to identifiable individuals. Such information, he argued, can still be used in ways that have an impact on individuals: the aggregated information can be used to classify people into groups; those groupings can then be used as the basis for decisions about pricing, marketing or other matters; and such decisions may have discriminatory or otherwise adverse effects on individuals. While such concerns may be valid, we do not think that the Privacy Act is the place to deal with them. The Privacy Act is concerned with the fair handling of information about individuals, not with aggregated information about groups of individuals. We discuss privacy of groups further below. If the uses of aggregated information described by Gunasekara are indeed a problem, they could be dealt with in other ways, such as through consumer legislation.

2.51 A somewhat different issue was raised by Professor Paul Roth of Otago University. He noted that a few overseas privacy laws provide that information may be "personal" even if it relates to two or more people, such as in the case of information about a family or household. He also referred to the case of *Sievwrights v Apostolakis*,[51] the implication of which, in Roth's view, is that:

> if there are two (or more) individuals who are referred to by a collective reference that does not identify one specific individual in particular, then an individual who is included in that collective reference may have a right to be granted that information as "personal information", even though it is not clearly "about" just that one individual alone. In principle, there is no reason why this logic should not also apply to disclosures, and possibly other complaints about breaches of the privacy principles.

We do not think that this issue of "individuation" ("the extent to which personal information must relate to one individual as opposed to a collection or aggregation of individuals") raised in Roth's submission is one that should be dealt with by amendment to the definition of "personal information". We prefer to leave it to be assessed case by case whether, in the particular circumstances, a reference to two or more people can be considered to be personal information about one of those people.

2.52 Another issue which we discussed in the issues paper concerns the extent to which an Internet Protocol (IP) address can be considered to be information about an identifiable individual.[52] Strictly speaking, an IP address identifies a computer, not a person, but some commentators and authorities overseas have taken the view that an IP address can be personal information. Our provisional view was that the issue of whether or not an IP address is personal information can only be decided in relation to the particular context in which that address is collected, held, used or disclosed, and that it could not be clarified by an amendment to the Privacy Act. This view was supported by participants in a roundtable discussion of internet privacy issues organised by InternetNZ in order to inform our review.

---

51 *Sievwrights v Apostolakis* HC Wellington CIV-2005-485-527, 17 December 2007. The Court found that a letter which used the surname "Apostolakis" and made no other reference to individuals contained personal information about Mrs Apostolakis even though the surname referred both to Mrs Apostolakis and to her husband.

52 Issues Paper at 54–55.

2.53 Overall, we think the "identifiable" element of the definition of "personal information" is capable of being clarified to some extent. For example, it can be stated clearly that information can be "personal information" if an individual can be identified from that information in combination with other information, but that such identification must be reasonably practicable and not simply theoretically possible. We considered whether such clarification could usefully be included in the Act itself, but concluded that to do so would involve significantly lengthening and complicating the current definition of "personal information". We think instead that the Privacy Commissioner could usefully develop guidance material on the "identifiable" element of the definition. While the "identifiable" element is the one that could most usefully be clarified through guidance, in our view, it might well make sense for such guidance also to address the other elements of the definition. In recommending that the Privacy Commissioner develop guidance material on this issue, we are conscious of the caveats with regard to guidance discussed above. Guidance can assist agencies to work through the issues involved in assessing whether particular information is "personal information" or not, can give examples and can draw on relevant Privacy Commissioner opinions and Tribunal and court decisions. It is important, however, that it is not seen as a substitute for the provisions of the Act itself and that it is applied flexibly.

RECOMMENDATION

R4 The definition of "personal information" should not be amended, but the Office of the Privacy Commissioner should develop guidance with respect to the "identifiable" element of the definition.

Human tissue samples

2.54 There is one final issue about the definition of "personal information" that we raised in the issues paper. We discussed the status of human tissue samples under the Privacy Act, and asked whether they should be covered by the definition of "personal information". Our provisional view was that they should not be.[53] We consider that human tissue samples are not currently included in the definition of "personal information", although information derived from such samples will be. Privacy legislation in New South Wales expressly includes bodily samples in the definition of "personal information",[54] and the Australian Law Reform Commission and the Australian Health Ethics Committee have recommended that bodily samples should be included in the coverage of the Federal Privacy Act.[55] In New Zealand, however, there is already a significant

53 See discussion in ibid, at 57–60. For a recent discussion of this issue in relation to the Data Protection Act 1998 (UK), see Neil C Manson "The Medium and the Message: Tissue Samples, Genetic Information and Data Protection Legislation" in Heather Widdows and Caroline Mullen (eds) *The Governance of Genetic Information: Who Decides?* (Cambridge University Press, Cambridge, 2009) 15.

54 Privacy and Personal Information Act 1998 (NSW), s 4(2); Health Records and Information Privacy Act 2002 (NSW), s 5(2).

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

body of law governing human tissue,[56] and we do not think it would be helpful to further complicate matters by extending the scope of the Privacy Act to cover such tissue. Most submitters who commented on this issue agreed with our view, and said that any reform in this area should be carried out through other legislation, such as the Human Tissue Act 2008. Nor did most submitters consider that any clarification was needed with regard to the Privacy Act's coverage of genetic information or other information derived from human tissue samples. We conclude that no reform is needed in this area. It is also worth noting that the Privacy Commissioner is not constrained from commenting on matters relating to human tissue samples or bodily privacy generally under the Commissioner's broad functions relating to "individual privacy" (as discussed in chapter 5).

"Individual"

2.55 As we have already mentioned, for information to be "personal information" under the Privacy Act, it must be about an identifiable "individual". "Individual" is defined as meaning "a natural person, other than a deceased natural person". Thus, information about artificial legal persons (such as companies) and other collective entities, and about deceased persons (albeit with some exceptions, discussed below), is not "personal information" and is not covered by the Act. In the issues paper we asked whether these exclusions from the Act's coverage should continue in their current form, be modified, or be removed.

Deceased persons

2.56 There are currently three exceptions to the general position that the Privacy Act does not apply to information about deceased persons. 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 (BDMRRA). For convenience, we will refer to this as "deaths register" information, using the term "deaths register" to include all the various forms in which the Registrar-General of Births, Deaths and Marriages maintains information about deaths pursuant to the BDMRRA. Secondly, an agency may refuse to provide access to information requested pursuant to privacy principle 6 if the disclosure of that information "would involve the unwarranted disclosure of the affairs of another individual *or of a deceased individual*".[57] Thirdly, the Act provides that, for the purposes of the issuing of any code of practice relating to health information, privacy principle 11 (disclosure) shall be read as if it applies in respect of both living and deceased

56 See especially Human Tissue Act 2008 and regulations made under that Act; Health and Disability Commissioner Act 1994, and the Code of Health and Disability Consumers' Rights, rights 7(9) and (10); Criminal Investigations (Bodily Samples) Act 1995; Coroners Act 2006, ss 47–56; provision for the making of regulations about the retention of bodily samples in Health Act 1956, s 121A.

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

individuals.[58] This provision is given effect by the Health Information Privacy Code (HIPC), which provides that rule 11 of the Code applies to health information about deceased individuals for a period of 20 years after death.[59]

2.57 We wondered whether these exceptions to the general principle that the Act does not cover information about the deceased could be tidied up somewhat, and in the issues paper we put forward some suggested reforms of the deaths register provision and the ground for refusing principle 6 access requests.[60] However, our suggestions would not have entirely eliminated the Act's coverage of information about deceased persons in either of these areas.

2.58 With regard to deaths register information, we suggested that the part of the definition of "personal information" that deals with deaths register information could be deleted, and such information could be governed solely by the BDMRRA (which might need some amendment as a result). We recognised, however, that deaths register information would still need to be considered to be personal information for the purposes of the information-matching provisions of the Act. There are a number of existing information matching programmes that involve matching of personal information with information on the deaths register. In some cases, such information matching will lead to adverse action (such as discontinuation of a benefit) being taken against a living person, due to a false match. Information matching involving deaths register information must, therefore, remain within the controls imposed by the Privacy Act. We recommend in appendices 1 and 2 that information matching should continue to be controlled under the Privacy Act, although we believe it should come within a new framework for information sharing.

2.59 In relation to the ground for refusing access where disclosure of information would involve the unwarranted disclosure of information about a deceased person, we suggested that this should be narrowed so that it applied only to health information about the deceased.

2.60 There was some support in submissions for these suggestions, but it was not strong, and a number of concerns were raised. With regard to the first suggestion, OPC questioned whether the BDMRRA can adequately substitute for the Privacy Act's role in relation to deaths register information. Both OPC and the Ombudsmen expressed concern about the implications of the second suggestion for the equivalent withholding ground under the OIA, which also allows information to be withheld to protect the privacy of deceased natural persons.[61] They felt that the OIA should continue to allow information about deceased persons to be withheld, as such information can be highly sensitive and its release can affect surviving family members. The Ombudsmen pointed out that requests for official information must often be considered under both the OIA and the Privacy Act because the information

58 Privacy Act 1993, s 46(6).

59 Health Information Privacy Code 1994, r 11(5) and (6). Health information about a deceased individual may, however, be disclosed if the disclosure is to, or is authorised by, the 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 individual's representative or certain other specified persons: r 11(1)(a), (b) and (f).

60 Issues Paper at 62–65.

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

requested is a mixture of information about the requester and other information. In such cases, inconsistency between the two Acts with respect to the withholding of information about deceased persons could create confusion. In light of the low level of support for change and the concerns raised in submissions, we have concluded that there should be no change to the inclusion of deaths register information in the definition of "personal information" or to the provision for information about deceased individuals to be withheld in response to access requests.

2.61 Our proposal in the issues paper with regard to the third way in which the Privacy Act currently applies to information about the deceased was rather different. We believe it is appropriate, in the health context, for information about deceased individuals to be protected against disclosure. Health information is particularly sensitive, and has traditionally been protected by medical confidentiality after death. Thus, we support the provision in the HIPC with regard to disclosure of health information about deceased individuals, as required by section 46(6) of the Act.

2.62 In the issues paper we proposed going further and providing in the Act that any code of practice made under the Act may apply any of the privacy principles to information about deceased persons. There was a significant level of support for this proposal in submissions, and OPC considered that it "might provide a measured and tailored approach" to privacy of information about deceased persons. We continue to support this proposal, which we see as allowing the principles of the Act to apply to information about the deceased in particular contexts and in ways that are appropriate to those contexts. To be clear, we are not proposing the making of a generic code about deceased persons' information, but rather that sector-specific codes should be able to apply to information about the deceased when appropriate. We are unable to say whether such a provision is ever likely to be used, especially given that few codes have so far been developed. In the issues paper we gave the banking sector as an example of one in which, if a code for the sector were to be developed, it could be appropriate to cover information about deceased persons, since confidentiality in banking (as in health) continues after death. No privacy code for the banking sector is currently under contemplation, however. The amendment we propose would also allow the existing codes to apply any principle to information about deceased persons, and in this respect we note the Privacy Commissioner's recommendation that principle 5 (security) should apply to health information of the deceased under the HIPC.[62]

2.63 We asked in the issues paper whether there are any other ways in which the Privacy Act should be amended to extend its application to information about deceased persons.[63] However, we indicated that we were not inclined to extend the Act's coverage of information about the deceased, apart from the provision about codes of practice that we have just discussed, and nothing in the submissions has caused us to change this view. As a matter of good practice rather than law, agencies can already handle information about deceased persons in accordance with the principles of the Act where appropriate.

62 *1st Supplement to Necessary and Desirable* at recommendation 75A.

63 Issues Paper at 66–68.

2.64 There is one further matter concerning information about deceased persons which we raised in the issues paper: survival of Privacy Act complaints after death. This issue concerns situations in which an individual suffers an alleged privacy breach while still alive and complains to the Privacy Commissioner, but dies before the complaints process has been completed.[64] In the case of *Yakas v Kaipara District Council*,[65] 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 in the Tribunal on his deceased mother's behalf. The Tribunal concluded that it did not have jurisdiction to hear the complaint, on the grounds that the right to bring complaints to the Tribunal, other than those brought by the Director of Human Rights Proceedings, is limited by section 83 to "aggrieved individuals", and that deceased persons are excluded from the definition of "individual". This interpretation of the Act has been questioned.[66] The general rule about survival of causes of action is contained in section 3(1) of the Law Reform Act 1936, which provides that on the death of a person all causes of action vested in that person survive for the benefit of his or her estate. The subsection provides for only two exceptions to this general survival rule: "causes of action for defamation or for inducing one spouse to leave or remain apart from the other". No doubt the rationale for these two exceptions is the intensely personal nature of the wrong. It can no doubt be argued that breach of privacy is equally personal and should likewise be exempted, but the exceptions to the rule in section 3(1) are very specific and very clear, and breach of privacy is not one of them.[67]

2.65 The question is whether the same rule should apply to breaches of the Privacy Act and to the remedial process for which it provides. It seems wrong in principle that an agency should be able to escape being held to account for a privacy breach against a person who was living at the time the breach occurred, simply because the person subsequently dies. Investigation of the complaint may lead to the discovery of systemic problems which can be corrected for the benefit of others. We therefore proposed in the issues paper that the Privacy Act should be amended to make it clear that section 3(1) of the Law Reform Act 1936 applies to causes of action under the Privacy Act. One submitter opposed this proposal on the grounds that a cause of action under the Privacy Act is particular to the individual, and should die with him or her. In this submitter's view, the damage from an interference with privacy is analogous to the damage to reputation in defamation cases, which cannot be continued after death. However, we consider that the flexibility of the Privacy Act is such that the fact of the complainant's death can be taken into account in deciding on an appropriate remedy. It may not be appropriate to award or negotiate damages because the direct sting to the complainant has gone, but remedies such as an apology or an agreement or order to take remedial action to address systemic problems could still be appropriate. Most submissions that addressed this question supported the Commission's proposal. Then Human Rights Review Tribunal Chair Royden Hindle suggested,

64 Ibid, at 70–71.

65 *Yakas v Kaipara District Council* [2004] NZHRRT 10.

66 Paul Roth *Privacy Law and Practice* (looseleaf ed, LexisNexis) at [PVA83.4(c)] [*Privacy Law*].

67 In 1977 the Committee on Defamation recommended a change in the law to give the family of a deceased person the right to sue for defamation in certain cases, but the recommendation was not accepted: Committee on Defamation *Recommendation on the Law of Defamation: Report of the Committee on Defamation* (Wellington, 1977) at 99.

however, that it could be useful if the Act also specified the point at which a cause of action under the Privacy Act should be regarded as having "vested" in the complainant (to use the language of the Law Reform Act 1936).

2.66 We recommend that causes of action under the Privacy Act should survive the complainant's death, for the benefit of his or her estate, in accordance with section 3(1) of the Law Reform Act 1936. This raises the question of the time that the cause of action accrues so that it becomes transmissible.

2.67 In a court setting, "a cause of action accrues when every fact exists which it would be necessary for the plaintiff to prove in order to support his or her right to the judgment of the court".[68] That will differ according to whether or not damage is a required element of the cause of action.

2.68 Privacy complaints are at first sight different from cases in court. The primary goal is to resolve them without litigation. Only a few proceed to the judicial body, the Human Rights Review Tribunal. In essence, however, the aim of all the processes provided for in the Privacy Act is to provide satisfaction for a person who has been wronged by a breach of the law. Even in areas of law which are more in line with the classic court model there are often early attempts to mediate. Sometimes consideration of that solution is mandatory, employment cases being the classic example.[69]

2.69 So, while one might have a rule that a "cause of action" under the Privacy Act survives for the benefit of the complainant's estate only when proceedings have been commenced in the Tribunal, a more rational solution would seem to be to provide that the cause of action in the present context accrues at the time the requirements of section 66(1) of the Privacy Act are satisfied; that is, there is a breach of privacy within paragraph (a) of that section, and the breach has caused, or may cause, harm within paragraph (b). That way, whether the complaint is settled in the early stages, proceeds to further investigation, or eventually reaches the Tribunal, the family can feel that the deceased aggrieved individual has been vindicated, and the infringing agency does not escape the consequences of its actions. If a case arises where the death of the aggrieved person would make further investigation pointless, section 71 of the Act gives the Commissioner adequate power to decline to proceed.

RECOMMENDATION

R5 The Privacy Act should provide that codes of practice may apply any of the privacy principles to information about deceased persons.

RECOMMENDATION

R6 Causes of action under the Privacy Act should survive the complainant's death, for the benefit of his or her estate. A "cause of action" should be defined as accruing at the time the requirements of section 66 of the Act are met.

68 Stephen Todd "Discharge of Liability" in Stephen Todd (ed) *The Law of Torts in New Zealand* (5th ed, Brookers, Wellington, 2009) 1153 at 1163.

69 Employment Relations Act 2000, s 159.

Corporations and groups

2.70 Because the definition of "individual" in the Privacy Act is limited to natural persons, the Act does not apply to information about legal persons (corporations) or unincorporated groups. This is consistent with the approach of most information privacy laws overseas, although some countries do extend privacy rights to corporations, at least in part.[70]

2.71 In the issues paper, we stated that we do not favour extending the Privacy Act to cover corporations for the following reasons:

- Privacy is a human right, based on protection of individual dignity.
- While corporations can be affected by misuse of their information, the harms suffered are fundamentally different from those suffered by individuals through breaches of their privacy.
- Those interests of corporations that are akin to privacy are already protected by other areas of law, including breach of confidence, defamation, intellectual property, and laws criminalising various forms of surveillance and theft of information.
- In return for the protections that come with their legal status, corporations take on obligations of transparency (that is, obligations to make certain information about themselves publicly available). They are publicly registered and governed by statute. Such characteristics of corporations limit the extent to which they can claim that information about them is "private".
- Including corporations in the Privacy Act's coverage would give rise to uncertainty, practical difficulties about the application of the privacy principles, and compliance costs.

Despite this view, we did seek submissions on the specific question of whether corporations should have rights of access and correction under principles 6 and 7, particularly in the field of credit reporting.

2.72 Most submitters were opposed to any extension of the Privacy Act to cover information about corporations, mainly on the ground that it would be inappropriate to do so in human rights legislation. A number of submitters also agreed with a point that we had made in the issues paper: that granting access rights to corporations would allow them to gather information about them held by their competitors, including information about their competitors' attitudes to them and strategies for competing with them. The credit reporting companies Veda Advantage and Dun & Bradstreet opposed giving corporations access and correction rights in the credit reporting field. They noted that it is in credit reporters' interests to have accurate information, and that they already provide for access and correction in relation to corporations' credit records. In their view, however, it would not be appropriate for the Privacy Act to provide for such access and correction rights, and there is no call for such a change. A similar point was made by the financial institution ANZ New Zealand. In light of these submissions, we remain of the view that information about corporations should continue to be excluded from the coverage of the Privacy Act.

70 See discussion in Issues Paper at 72–74.

2.73 We also briefly discussed in the issues paper the question of privacy and unincorporated groups. We do not see how a group right to privacy could be recognised within the Privacy Act framework. The Act is based on the rights of individuals to control information about themselves, and a collective right to privacy could not be recognised without fundamentally changing the nature of the Act. We also note that unincorporated bodies cannot sue in tort. However, a group of individuals may have common interests that could be recognised by the law. Such recognition could be achieved by means of a representative complaint on behalf of a group of individuals, each of whom would be able to bring a complaint individually if he or she chose to do so. In chapter 6 we recommend that the Privacy Act should make better provision for representative complaints. We think that this is as far as the Privacy Act can go towards recognising the privacy interests of groups.

2.74 One other issue raised in the issues paper concerns the question of whether information about a corporation can, in some circumstances, be information about an individual.[71] In the Tribunal case *C v ASB Bank*,[72] C was the sole director and owner of all but one share in a business. He used the company's bank account for personal as well as business transactions, and after he and his wife separated, his wife obtained copies of the company's bank statements from the bank. C complained about the bank's disclosure, which he had not authorised, and he submitted that the bank statements were personal information. Even though the information was, on its face, about the company, C argued that it was transformed into personal information by factors such as the one-person nature of the company, the use of the account partly for personal transactions, and the fact that his wife wanted the information in order to learn about him, not about the company. The Tribunal disagreed, ruling that the information was about the company, not about C, and was therefore outside the scope of the Act.

2.75 In the issues paper we said that the very strict interpretation in *C v ASB Bank* seemed out of character with the Privacy Act's flexible approach, and we proposed that the 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. There was a reasonable amount of support for the proposal in the issues paper, but also some quite strong opposition. Arguments in support did not go beyond those made in the issues paper. The main argument against the proposal was that people who have chosen to structure their affairs through the vehicle of a company must accept the consequences of that decision. There was also concern that, by "piercing the corporate veil", the proposal departed from established principles of company law. While the proposal would have applied only in limited circumstances, it would be a significant departure from the general principle that the Privacy Act does not apply to information about corporations, and in the absence of consensus on this issue we have decided that the proposal should not proceed.

71 Ibid, at 74–76.

72 *C v ASB Bank Ltd* Complaints Review Tribunal 21/97, 26 August 1997.

2.76 We also asked whether the Act needed to clarify the circumstances in which information about a trust can be personal information. We have no recommendations to make about information relating to trusts, since no issues were raised about such information in submissions.

"Collect"

2.77 The Privacy Act defines "collect" as follows: "**Collect** does not include receipt of unsolicited information". Thus, unsolicited information will not be "collected" for the purposes of the Act, and will therefore not be covered by the collection principles (privacy principles 1 to 4). We refer to the exclusion of unsolicited information from the meaning of "collect" as "the unsolicited information exception". It is important to note that the definition of "collect" does not affect interpretation of privacy principles 5 to 12, which do not use the word "collect". Principles 5 to 11 deal with information that an agency "holds", and principles 10 and 11 also refer to the purposes for which information was "obtained". The Act does not define "obtained", but it seems clear that it covers situations in which information comes into the possession of an agency, regardless of whether the information was collected by the agency or was unsolicited. Neither "unsolicited" nor "solicit" are defined in the Act. It does not seem to be common in information privacy laws overseas to define "collect", or to provide that "collection" does not include receipt of unsolicited information.[73]

2.78 In the issues paper we discussed possible areas of uncertainty with regard to the meaning of "unsolicited", and therefore of "collect".[74] In our view, to "solicit" information is to request or invite it; "unsolicited" information is information that has not been asked for.[75] Some types of information are clearly unsolicited: for example, information sent to an agency by mistake, or information sent to an agency by a third party without the agency requesting it (such as a tip-off that an individual is engaging in unlawful activity). However, in other cases the unsolicited information exception may give rise to uncertainty about whether information has been collected or not:

- Privacy law expert Professor Paul Roth has questioned whether surveillance by means of a recording or monitoring device is collection for the purposes of the Act. In Roth's view, such surveillance of an individual is not collection because the information is not solicited in the sense of a request for the information being made to the individual.[76]
- It may be unclear whether agencies, or sections within agencies, that exist in order to receive inquiries or complaints "solicit" the information that is provided to them. Examples include customer service or complaints departments, or complaints bodies such as professional disciplinary tribunals.
- Some information is generated within an agency, rather than being collected from an external source. One example is the outcome of a completed

73 However, see discussion of some relevant provisions in Australian Federal and New South Wales legislation in Issues Paper at 76–77.

74 Ibid, at 77–79.

75 See discussion of the meanings of "solicit" and "unsolicited" in ibid, at 80.

76 Roth *Privacy Law*, above n 66, at [PVA2.5].

disciplinary process;[77] another is information that is automatically generated in the course of a transaction (such as a phone company's records of calls made by its subscribers).

2.79 It is mainly the application of the definition of "collect" to the first of these situations, the collection of information by means of surveillance devices, that is of concern to us. With regard to complaints bodies and other similar agencies or sub-agencies, we think they are already covered by the definition. Where an agency asks customers for feedback or holds itself out as being the appropriate body to receive complaints, it is soliciting information in our view, even if it is not specifically soliciting each individual piece of information it receives. On the other hand, the status of internally-generated information could be unclear even without the unsolicited information exception: it is certainly open to debate whether an agency's record of the fact that a particular decision was taken or that a particular transaction took place constitutes a collection of that fact.

2.80 In the case of an agency obtaining information by means of a surveillance device, we think that the current definition of "collect" introduces an unhelpful ambiguity. Without the unsolicited information exception, there could be little doubt, in our view, that a device such as a CCTV camera could be used to "collect" personal information. We find it difficult to see, however, how information recorded by a CCTV camera that sits passively recording images of people within a particular area can be said to have been "solicited" from the individuals concerned. Those individuals have not been asked if they want to be filmed; they may not even be aware that they are being recorded. If the camera is hidden, the unsolicited nature of the information obtained is even clearer.

2.81 We emphasise that we think the current definition is not *intended* to exclude the obtaining of information by means of surveillance devices from the definition of "collect". The purpose of and background to the Act suggest that surveillance should be considered to be a form of collection,[78] and both the Privacy Commissioner and the Tribunal have taken the view that surveillance devices can be used to "collect" information. There is, however, a Court of Appeal decision that lends limited support to Professor Roth's contention about the application of "collect" to the use of surveillance devices,[79] and in any case we think that the matter should be put beyond doubt.

2.82 In the issues paper we considered a number of options for clarifying the meaning of "collect", and proposed that the definition should simply be deleted.[80] We considered that the natural and ordinary meaning of "collect" would be sufficient to cover the types of activity that are intended to be covered by the

77 See for example *Boyle v Manurewa RSA Inc* [2003] NZHRRT 16. The Tribunal found (at [31]) 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.

78 See, for example, the Explanatory Memorandum to the OECD Privacy Guidelines, at [52], 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".

79 *Harder v Proceedings Commissioner*, above n 45. The Court decided in this case that an unsolicited phone call was not "collected" simply by virtue of it having been recorded. The decision is of limited relevance to a situation such as an agency deliberately installing a camera and using it to obtain information about people in a particular area.

80 Issues Paper at 81–82.

collection principles, while excluding situations in which an agency has taken no steps to acquire the information in question.[81] However, we also put forward the alternative options of amending the definition of "collect" (which could be done in a number of ways), or clarifying the definition by means of guidance from the Privacy Commissioner.

2.83 Most submitters who commented on this issue supported our proposal to simply delete the definition of "collect". Points made by submitters included that:

- the proposed change would bring the New Zealand Privacy Act into line with Australian privacy law;
- the proposal would ensure that unsolicited information is covered by the Privacy Act;
- the ordinary meaning of "collect" should suffice, and the reference to "unsolicited" information is unhelpful as once the information is held most of the privacy principles apply anyway;
- the current definition is unhelpful, and attempts to provide further clarification could simply give rise to new definitional problems; and
- information collected by means of surveillance devices should clearly fall within the coverage of the Act.

Several other submitters did not agree that the definition should be deleted, but did agree that it should be amended to make its scope clearer (particularly in relation to information obtained using surveillance devices). Only two submitters opposed any change to the current definition, because they wanted to ensure that unsolicited information continues not to be "collected" for the purposes of the Act.

2.84 In its submission, OPC said that:

> given that the Act has been in effect for 17 years, simply deleting the definition would be confusing since it may not be clear whether previous interpretations are intended to be changed or continued. If amendment is warranted, statutory clarification would be a better course.

OPC disagreed with the proposition that, where information is gathered about people who happen to be in a particular space and no request for information is made to any individual, the information is "unsolicited". If clarification is considered necessary, OPC suggested it may be useful to define "unsolicited" narrowly, so as to exclude only:

> those situations where the agency cannot in practice be held accountable for informing the individual about the collection, for the manner of collection, or for justifying why it needs the information. For instance, "unsolicited information" can be defined as "information that comes into the possession of the agency in circumstances where the agency has taken no active steps to acquire or record that information".

2.85 We remain of the view that the meaning of "collect" should be made clearer, and this view has been broadly supported by submitters. If we were starting with a blank slate, we think the ordinary meaning of "collect" would suffice to exclude information that comes into an agency's possession but that the agency did not

81 See discussion of the meaning of "collect" in ibid, at 79.

seek or invite. However, we take OPC's point that simply deleting the definition at this point, after it has been in existence for 17 years, could cause uncertainty. It might be assumed that, by deleting the unsolicited information exception, Parliament was indicating that all unsolicited information should in fact be covered by the definition of "collect". We therefore recommend that the definition of "collect" should be amended rather than deleted. The effect of the amendment should be to exclude from the meaning of "collect" situations in which an agency has taken no active steps to acquire or record information.

RECOMMENDATION

R7 The definition of "collect" should be amended to provide that situations in which an agency has taken no active steps to acquire or record information are excluded from the definition.

"Publicly available publication"

2.86 We asked in the issues paper whether there were any other terms used in the Privacy Act that needed to be defined, or whose definitions should be amended. We received few suggestions in submissions, and there is only one additional term whose definition needs clarification, in our view. We mentioned in the issues paper that the definition of "publicly available publication" could be amended to clarify its application to online information, but we did not examine this issue in any detail. This issue was discussed at a seminar on privacy and the internet organised for us by InternetNZ, and participants in that discussion felt that clarification of what "publicly available" means in the online context would be useful.[82] OPC's submission also suggested that consideration could be given to clarifying this issue, and an article on privacy and Web 2.0 attached to the submission from Professor Paul Roth of Otago University included a very helpful discussion of "publicly available" exceptions in New Zealand and overseas privacy laws.[83]

2.87 There are exceptions to principles 2, 10 and 11 in relation to information that is "publicly available information" or is in a "publicly available publication".[84] This means that, if information is "publicly available", it is not necessary to collect it directly from the individual concerned, or to use or disclose it only for the purpose for which it was obtained. The relevant definitions are as follows:

> **Publicly available information** means personal information that is contained in a publicly available publication
>
> **Publicly available publication** means a magazine, book, newspaper, or other publication that is or will be generally available to members of the public; and includes a public register

82 InternetNZ Privacy Roundtables (Wellington, 21–22 June 2010).

83 Paul Roth "Data Protection Meets Web 2.0: Two Ships Passing in the Night" (2010) 33 UNSWLJ 532 at 544–547 ["Data Protection"].

84 Privacy Act 1993, s 6, principles 2(2)(a), 10(a) and 11(b).

Since "publicly available information" is defined in terms of being contained in a "publicly available publication", the latter term is the key one. There are "publicly available" exceptions in information privacy statutes overseas, and these exceptions take a variety of forms. Professor Roth comments in his article on Web 2.0 issues that New Zealand's exception is unusually broad.[85]

2.88 The need to clarify the meaning of "publicly available publication" arises largely, though not exclusively, from the fact that the internet has made so much more information "publicly available". Because so much information is available on the internet, there is a lot of information that is potentially not protected by the Privacy Act because it is already "publicly available". In some cases the individual concerned will have had no role in making that information publicly available, or will have taken steps to make it available only to a limited audience. We discuss several issues about the definition of "publicly available publication" below. For convenience, we also discuss here the scope of the "publicly available" exceptions to principles 2, 10 and 11.

Websites and information in electronic form

2.89 The fact that websites and other electronic publications can be "publicly available publications" seems clear,[86] but we think it should be stated expressly in the definition. Overseas privacy laws use a variety of forms of words to include electronic publications, such as "whether in printed or electronic form" or "however published". "Website" could also be added to the list of forms of publication in the definition (as it is already in a similar definition in the Criminal Disclosure Act 2008).[87]

Information to which access is restricted

2.90 The question of whether or not information is "generally available to members of the public" is not always straightforward. Information can be publicly accessible to some extent, but subject to certain restrictions on access. One obvious example of an access restriction is that a publication may be available only on payment of a fee or subscription. The definition of "publicly available publication" already includes publications – books, magazines and newspapers – that are usually available for purchase, although they may also be available for free online or in public libraries. The Australian and New South Wales Law Reform Commissions have recommended that the definition of "generally available publication" (the equivalent term in Australian Federal and New South Wales privacy statutes) should be amended to clarify that a publication can be "generally available" whether or not a fee is charged for access to it.[88] The Australian Government has accepted this recommendation in relation to the

85 Roth "Data Protection", above n 83, at 545.

86 See *Personal Information on Internet was Publicly Available* [2010] NZPrivCmr 8, Case Note 212156; *Coates v Springlands Health Ltd* [2008] NZHRRT 17 at [79].

87 Definition of "publicly available publication", Criminal Disclosure Act 2008, s 6(1).

88 *For Your Information* at 333–335 (recommendation 6–7); New South Wales Law Reform Commission *Access to Personal Information* (NSWLRC R126, Sydney, 2010) at 30–31, 34 (recommendation 6).

Privacy Act 1988 (Cth).[89] We recommend that a similar amendment should be made to the definition of "publicly available publication" in New Zealand's Privacy Act. However, we think a form of words should be found that allows for the possibility that a particular publication may be so expensive that it cannot be said realistically to be publicly available. For example, various specialist academic or legal databases are available on payment of very substantial subscriptions that put them out of reach of members of the public generally.

2.91 There are a number of other ways in which access to publications may be limited, particularly online. For example, users of the social networking site Facebook can restrict access to all or parts of their profiles to people they have accepted as "friends", or to specific sub-groups of "friends". Similarly, some websites restrict access to certain information to people who have passwords (who might, for example, be members of a particular club or professional association that the website is about). Where information is available only to a small section of the public, we do not think that the information in question can be considered to be "generally available to members of the public".

2.92 It is difficult to lay down strict rules about information in a publication to which access is restricted, but we think that certain factors can be identified which should be considered in assessing whether or not information is publicly available. These factors include:

- the level of any fee or subscription that is charged for access;
- whether access is restricted by means of a password to certain authorised users;
- whether access is restricted to a limited audience chosen by the individual publishing the information (as in the case of limiting access to Facebook "friends"); and
- whether the information is published in encrypted form.

We considered whether factors such as these should be spelled out in the Act itself, but we think it would be better to deal with them in guidance from OPC, and we recommend that such guidance about the meaning of "publicly available publication" should be developed.

Public registers

2.93 The definition of "publicly available publication" currently expressly includes "a public register". "Public register" is defined in section 58 of the Privacy Act. A "public register" for the purposes of the Act is a register maintained pursuant to a legislative provision listed in Schedule 2 to the Privacy Act, or a document specified in that same Schedule. In our *Public Registers* report, the Law Commission noted that there are a number of registers that are provided for in statutes or regulations and that are at least partially open to the public, but that are not included in Schedule 2 to the Privacy Act.[90] In *Necessary and Desirable*,

89 *Enhancing National Privacy Protection* at 26. The Exposure Draft of new Australian Privacy Principles released by the Australian Government as part of its response to the ALRC report provides (cl 15) that a publication can be a "generally available publication" "whether or not it is available on the payment of a fee".

90 Law Commission *Public Registers: Review of the Law on Privacy Stage 2* (NZLC R101, 2008) at 22–23, 36 [*Public Registers*]. See also the list of statutory provisions for public registers in ibid, at 98–116.

the then Privacy Commissioner commented that a public register not included in Schedule 2 will only be a "publicly available publication" if it is a "publication that is or will be generally available to members of the public". He appeared to suggest that such registers would only fall within the definition if they were published in something like book form, and said that:[91]

> there exists a potential anomaly whereby information or documentation having very similar characteristics in terms of being publicly available may, depending upon certain formatting issues, perhaps fall outside the relevant definitions.

He did not recommend any amendment to the definition of "publicly available publication" to deal with this issue, however, since he had recommended elsewhere in *Necessary and Desirable* that a process should be undertaken to bring all statutory registers open to public search into the list in Schedule 2.

2.94 In *Public Registers*, the Law Commission has recommended that all public registers should be regulated primarily through their establishing statutes, and that consequently the public register provisions of the Privacy Act and the Act's definition of "public register" should be repealed.[92] For the time being, however, we assume that "public register" will continue to be a defined term in the Act. We do not see this as a problem in relation to the definition of "publicly available publication", since we think the definition is broad enough to include other registers that are open to public inspection. There is, however, a growing tendency for public registers to be only partially open to public search and inspection, or open only for certain purposes specified in their establishing statutes. Protection of privacy is one of the main reasons for restricting access to public registers. Public registers should continue to be expressly included in the definition of "publicly available publication", in our view, but they should be included only to the extent that the information in them is in fact "generally available to members of the public". The simplest way of making this clear is to move the words "public register" from the end of the definition, so that they appear instead before "or other publication".

An amended definition of "publicly available publication"

2.95 Taking the points made above into account, a new definition of "publicly available publication" might read as follows:

> **Publicly available publication** means a magazine, book, newspaper, website, public register, or other publication (whether in printed or electronic form) that is or will be generally available to members of the public, and can include a publication that is available on payment of a fee.

2.96 We note that the definition of "publicly available publication" in the Criminal Disclosure Act 2008 is similar to that in the Privacy Act, although unlike the Privacy Act definition it expressly includes websites.[93] If the definition in the Privacy Act is amended, consideration should be given to making a corresponding amendment to the definition in the Criminal Disclosure Act.

---

91 *Necessary and Desirable* at 52.

92 Law Commission *Public Registers*, above n 90, at 74–75, 89.

93 Criminal Disclosure Act 2008, s 6(1).

Amending the "publicly available" exceptions

2.97 In addition to the issues about the definition of "publicly available publication", discussed above, we are concerned about the breadth of the "publicly available" exceptions. Most privacy statutes in comparable jurisdictions overseas limit the scope of the exception in some way. For example, the exception may apply only where:

- publication of the information in question is required or authorised under statute;
- there are reasonable grounds for believing that the individual concerned provided the information or authorised its publication; or
- the collection, use or disclosure of the information is consistent with the purpose for which the information was published.

Participants in the InternetNZ forum particularly drew attention to provisions in overseas laws that state that personal information made publicly available for one purpose cannot be reused for another purpose. They saw merit in adopting this approach in New Zealand.

2.98 We think the scope of the "publicly available publication" exception to the use and disclosure principles (principles 10 and 11) should be narrowed. Reuse or disclosure that is inconsistent with the purpose for which the information was published, or that involves the use or disclosure of sensitive information that has been made publicly available without the authorisation of the individual concerned, can be harmful to individual privacy. To take an extreme example, if a person were to publish on a website sensitive personal information (personal medical records, for example) that had been obtained by hacking into a computer or through some other security breach, others should not be free to use or further disclose this information. Similarly, there have been incidents in which (usually after a relationship breakup) naked photographs of an individual are posted on a social networking site such as Facebook without that individual's consent.[94] The posting of such photographs should not give others licence to further use or disclose them.[95]

2.99 We therefore recommend that the "publicly available publication" exceptions to principles 10 and 11 should be amended to provide that the exceptions cannot be relied on if, in the circumstances of the case, it would be unfair or unreasonable to use or disclose personal information obtained from a publicly available publication. We do not see a need for an equivalent amendment to the exception to principle 2. The "publicly available" exception to principle 2 means that an agency does not need to collect information from the individual concerned if the information is contained in a publicly available publication. So long as any

94 See, for example, "Naked Photo Sends Jilted Lover to Jail" *Dominion Post* (Wellington, 13 November 2010) < www.stuff.co.nz > ; Chris Barton "Facebook Shows its Ugly Side" *New Zealand Herald* (Auckland, 20 November 2010) < www.nzherald.co.nz > .

95 The English Court of Appeal has suggested that some types of information are so sensitive that an expectation of privacy can remain in respect of such material even after it has been widely published. The Court thought that this was particularly true of photographs: *Douglas v Hello! Ltd (No 3)* [2006] QB 125 (CA) at [105]. For further discussion see John Burrows "Invasion of Privacy" in Stephen Todd (ed) *The Law of Torts in New Zealand* (5th ed, Brookers, Wellington, 2009) 845 at 861–862; Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009) at 138.

information collected in this way is protected against use or disclosure that would be unfair or unreasonable, we think there is no need to limit the collection of information from publicly available publications.

RECOMMENDATION

R8 The definition of "publicly available publication" should be amended to make it clear that:

- it includes websites and other material published in electronic form;
- a publication can be publicly available even if a fee is charged for access; and
- public registers are included only to the extent that they are generally available to the public, by moving the reference to "a public register" from the end of the definition, so that it appears instead before the words "or other publication".

RECOMMENDATION

R9 The Office of the Privacy Commissioner should develop guidance material with respect to the meaning of "publicly available publication", focusing particularly on information to which access is restricted to some extent.

RECOMMENDATION

R10 The scope of the "publicly available publication" exceptions to principles 10 and 11 should be narrowed, so that the exceptions cannot be relied on if, in the circumstances of the case, it would be unfair or unreasonable to use or disclose personal information obtained from a publicly available publication.

Chapter 3
Privacy principles

3.1 Like information privacy legislation in other countries, the Privacy Act sets out principles for regulating the handling of personal information. There are 12 "information privacy principles", which are set out in section 6 of the Act. These principles are fundamental to the Act's operation, so it is essential for any review of the Act to consider whether their effectiveness can be improved.

3.2 We think the privacy principles have generally worked well, and are consistent with internationally-accepted principles for the fair handling of personal information. Because of this, and because people have now worked with the current principles for almost 20 years, our approach to reform of the principles involves making improvements to the existing principles, rather than starting again from scratch.

3.3 We have recommended in chapter 2 that the Privacy Act should continue to take an open-textured, principles-based approach to regulating informational privacy, rather than moving towards a rules-based system. In keeping with an open-textured approach, we believe 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 (although 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 clear and simple, so that they are easy to understand and apply.

The above criteria have guided our decisions on reform of the privacy principles.

A BRIEF SUMMARY OF THE PRINCIPLES

3.4 The privacy principles are set out in full in appendix 3. In brief, the principles are as follows:

- *Principle 1:* An agency must not collect personal information unless the collection is necessary for a lawful purpose connected with the agency's functions or activities.
- *Principle 2:* Agencies must collect personal information from the individual to whom the information relates, unless certain exceptions apply.
- *Principle 3:* When personal information is collected from the individual to whom it relates, that individual must (unless certain exceptions apply) be

made aware of such matters as the fact that the information is being collected, the purpose for which it is being collected, and the intended recipients of the information.

- *Principle 4:* Agencies must not collect personal information by means that are unlawful or unfair, or that intrude unreasonably upon an individual's personal affairs.
- *Principle 5:* Agencies that hold personal information must take steps to keep it secure against loss; unauthorised access, use, modification or disclosure; or other misuse.
- *Principle 6:* An individual is entitled to obtain confirmation from an agency as to whether or not the agency holds that individual's personal information and, if the agency does hold such information, the individual is entitled to have access to it. However, there are certain grounds on which an agency can refuse to provide an individual with access to his or her personal information.
- *Principle 7:* If an agency holds an individual's personal information, the individual is entitled to request that the agency correct that information. If the agency does not agree to correct the information, it must take reasonable steps (if requested to do so) to attach to the information a statement of the correction sought but not made.
- *Principle 8:* Before it uses personal information, an agency must take reasonable steps to check that the information is accurate, up to date, complete, relevant and not misleading.
- *Principle 9:* Agencies must not retain personal information for longer than is required for the purposes for which the information may lawfully be used.
- *Principle 10:* Personal information obtained by an agency for one purpose must not be used for another purpose unless certain exceptions apply.
- *Principle 11:* An agency must not disclose personal information unless certain exceptions apply.
- *Principle 12:* This principle places restrictions on the use of "unique identifiers" such as IRD numbers or credit card numbers. The principle restricts the ways in which agencies may assign such numbers to individuals, and the circumstances in which they may require individuals to disclose such numbers.

3.5 Stating the principles in this way is somewhat misleading with regard to those principles that include exceptions: principles 2, 3, 6, 10 and 11. The exceptions to these principles modify the application of the principles in important ways. It is impossible to summarise the exceptions, but they allow agencies not to comply with the basic principle for such reasons as that non-compliance is necessary to protect interests such as health, safety and maintenance of the law; that compliance would not be reasonably practicable in the circumstances; or that the individual to whom the information relates has authorised non-compliance. The exceptions to principle 6 are set out in sections 27 to 29 of the Act, whereas the exceptions to the other principles are included in the body of

the principles themselves. Even those principles that do not include exceptions are generally qualified in some way, particularly by providing that an agency must take only such steps as are reasonable in the circumstances.

3.6 For the purposes of discussion in this chapter, we have grouped the principles as follows: collection (principles 1 to 4); security, accuracy and retention (principles 5, 8 and 9); access and correction (principles 6 and 7); use and disclosure (principles 10 and 11); and unique identifiers (principle 12). At the end of the chapter we discuss whether any new principles are needed.

STRUCTURAL CHANGES TO THE PRINCIPLES

3.7 In the issues paper we asked about combining or deleting existing principles, or making structural changes to the exceptions to the principles.[96] Most submitters did not favour such changes, and we recommend that the basic structure of the principles should not be changed.

3.8 A few submitters thought that principles 10 and 11 (use and disclosure) could usefully be combined, but in the absence of strong support for such a change we think that they should remain separate. Arguments put forward in submissions against combining principles were that people are familiar with the existing principles, that all of the principles serve a useful purpose, that keeping them separate helps to make them user-friendly, and that combining principles in the Act could cause problems for the rules in codes of practice.

3.9 We asked in the issues paper whether principle 12 (unique identifiers) should be removed from the principles and placed elsewhere in the Act. Principle 12 seems different in character from the other principles, being more specific and prescriptive. However, there was very little support for such a change.

3.10 The idea of moving the exceptions to principle 6 (reasons for refusing access) from sections 27 to 29 into the body of principle 6 itself was supported by a few submitters, but most submitters saw no reason for change. The main argument against moving the provisions of sections 27 to 29 into the body of principle 6 is the length of these exceptions, and we think it is better to leave them where they are. We note, however, that the Privacy Commissioner has made useful recommendations about the restructuring of sections 27 to 29 to make them easier to use.[97]

COLLECTION PRINCIPLES

3.11 Principles 1 to 4 are concerned with the collection of information. We have discussed the definition of "collect" in chapter 2. Principle 1 says that an agency is to collect personal information only for a lawful purpose connected with the agency's function or activity, and is to collect only such information as is necessary for that purpose. Principle 2 provides that, in most cases, agencies must collect personal information from the individual to whom it relates, while principle 3 says that when information is collected from an individual, he or she must usually be informed of certain matters. Principle 4 states that agencies shall not collect personal information by unlawful, unfair or unreasonably intrusive means. Principles 2 and 3 are subject to a number of exceptions, but there are no exceptions to principles 1 and 4.

96 Issues Paper at 85–87.

97 *2nd Supplement to Necessary and Desirable* at 9, 16–18.

Principle 1 – purpose of collection

3.12 The concept of "purpose" is fundamental to the privacy principles, and it is principle 1 that requires agencies to have a purpose for which they are collecting personal information. We asked in the issues paper whether greater clarity was needed in relation to defining the purpose of collection, and whether principle 1 should be amended to require that the collection of personal information must be *reasonably* necessary for the purpose.

3.13 There was no clear pattern in the submissions on the question of defining purpose. On the one hand, some submitters did think that agencies may currently be able to get away with overly-broad or vague purposes for collection. The Office of the Privacy Commissioner (OPC) said that it had encountered many instances in which agencies are not transparent with respect to their purposes of collection: for example, purposes may not be documented, or may be characterised in broad and vague terms. OPC saw the solutions as lying not with an amendment to principle 1, but in the provision of better enforcement tools (discussed in chapter 6) and the introduction of a new openness principle (discussed later in this chapter). On the other hand, a couple of government departments asked in their submissions for greater flexibility with regard to definition of purpose. They wanted to be able to change or expand the purpose for which they hold information, rather than being tied to the purpose for which the information was originally collected.

3.14 On the question of reasonableness, some submitters thought that it could be helpful to spell out that collection should be *reasonably* necessary, but a larger number of submitters did not support such an amendment. Those who opposed the change said that it would make no difference as the Tribunal has already interpreted "necessary" as meaning "reasonably necessary",[98] or that adding the word "reasonably" to principle 1 would simply raise questions about what "reasonableness" means. A government department pointed out that "necessary" is also used elsewhere in the privacy principles, and that if "reasonably" is added only in principle 1 it could be seen as imposing a different threshold of necessity from that in the other principles.

3.15 We have concluded that no change is needed to principle 1. We do not believe it is possible to amend principle 1 to require agencies to define their purposes for collection more precisely. At the same time, the suggestion that agencies should be able to change the purpose for which they hold personal information from that for which the information was collected is not one that we can support. Allowing agencies to change purpose unilaterally would create such a large hole in the Act as to render it almost meaningless. If agencies wish to use information for a purpose other than that for which they collected it, they should seek the authorisation of the individuals concerned, or make use of one of the other exceptions. On the question of reasonableness, we are persuaded by the prevailing view in submissions, that requiring collection to be "reasonably" necessary would add nothing and might in fact lead to greater uncertainty.

98 *Lehmann v CanWest Radioworks* [2006] NZHRRT 35 at [49]–[50].

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

3.16 Principles 2 and 3 are closely related, and have many exceptions in common, so we consider them together. Principle 3 applies only if personal information has been collected from the individual concerned, in accordance with principle 2. Thus, if an agency has not collected the information from the individual concerned (because one of the exceptions to principle 2 applies), there is no obligation to notify the individual to whom the information relates of the matters set out in principle 3.

Collection "directly" from the subject

3.17 Principle 2 requires agencies to collect personal information "directly" from the individual concerned, unless one of the exceptions applies, and principle 3 applies only where information has been collected "directly" from the individual concerned. Professor 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.[99] In response, the Privacy Commissioner has recommended that the word "directly" be deleted from principle 3.[100] In the issues paper we supported this recommendation, and said that "directly" should also be deleted from principle 2. We commented that such a change would help to remove any ambiguity, and that "directly" does not seem to serve any useful purpose.

3.18 Most submitters supported our proposal to delete "directly" from principles 2 and 3. However, IHC opposed the proposal out of concern that it might open the door too wide to the collection of personal information through intermediaries. The Ministry of Health was also concerned about the proposed change, noting that the Ministry collects personal information from health providers, who have in turn collected that information from the individuals concerned. In the first instance those health providers have generally collected the information for purposes related to their own activities, and have not collected it as agents for the Ministry. The Ministry was concerned that, if "directly" were to be deleted, the Ministry could be considered to be collecting personal information from the individuals concerned, and could therefore be responsible for the matters covered by principle 3.

3.19 Our view on this issue is unchanged from that put forward in the issues paper. We do not think that "directly" adds clarity to principles 2 and 3, and we consider that deleting it will have no effect on a situation like that described by the Ministry of Health. In that situation, the Ministry is clearly not collecting information from the individual concerned, and is not responsible for the notification required by principle 3. In collecting information from a third party, the Ministry must be relying on one of the exceptions to principle 2, and again we think that the deletion of "directly" will make no difference to the assessment of whether or not information can be collected from someone other than the individual concerned. At the same time, its deletion should help to clarify the position with respect to a situation in which information is collected by means of a device such as a camera or audio recorder. It is arguable that, if an agency

99 Paul Roth *Privacy Law and Practice* (looseleaf ed, LexisNexis) at [PVA6.6(c)] [*Privacy Law*].

100 *3rd Supplement to Necessary and Desirable* at 2–3 (recommendation 19A).

sets up a CCTV camera to record people in a public place, personal information about individuals in that place is not being collected "directly" from them. The information is, however, clearly being collected from those people as opposed to being collected from third parties.

RECOMMENDATION

R11 The word "directly" should be deleted from principles 2(1) and 3(1).

Unsolicited information

3.20 The definition of "collect" in the Act currently excludes "receipt of unsolicited information". We discussed this definition in chapter 2, and recommended that it be amended to deal with some uncertainty about the meaning of "unsolicited". We do, however, think that personal information should continue to be considered not to have been "collected" for the purposes of the Act if the agency has taken no active steps to obtain that information. This raises the question of how such unsolicited information should be treated. In the issues paper,[101] we proposed to amend principle 2 by providing that unsolicited information must either be destroyed or, if it is retained, handled in compliance with all the relevant provisions of the privacy principles, as if the agency had taken active steps to collect the information. This proposal was based on a recommendation of the Australian Law Reform Commission (ALRC), which has been accepted by the Australian Government.[102] We also proposed that principle 2 should provide that an agency must not retain unsolicited information that it would have been unlawful for it to have collected.

3.21 Although more submitters supported our proposals than opposed them, few arguments were put forward in support. Those who opposed the proposals were concerned about their practicability, and about the implications for use of "tip off" information about fraud or other wrongdoing. With regard to the proposal that the Act should provide that agencies must not retain unsolicited information that they could not have lawfully collected, a number of submitters said that agencies would not always be in a position to judge this, as they might not be able to determine the circumstances in which the information was collected. Moreover, it was argued, agencies with a law enforcement role must be able to act on information concerning breaches of the law, regardless of how that information was obtained.

3.22 In light of the fairly lukewarm support for our proposals, and the strong opposition from a number of submitters, we now recommend that principle 2 should not be amended to deal expressly with unsolicited information. In any case, we think that the Act already requires agencies to treat unsolicited personal information with care. Principles 5 to 9 deal with information that an agency "holds", and make no reference to collection. Thus, they cover any information an agency has decided to retain, whether that information was originally solicited

101 Issues Paper at 91.

102 *For Your Information* at 726 (recommendation 21–3); *Enhancing National Privacy Protection* at 41; Australian Government "Australian Privacy Principles: Exposure Draft" (2010) principle 4 – receiving unsolicited information.

or unsolicited. Principle 9 requires that information be kept for no longer than is required for the purposes for which the information may be lawfully used, which means that if the agency does not have a lawful purpose for that information it must destroy or otherwise dispose of it. Principles 10 and 11 refer to the purposes for which personal information was "obtained". "Obtaining" information would appear to include both collecting information and receiving unsolicited information. Thus, in our view principles 5 to 11 already apply to unsolicited personal information which an agency decides to retain. In deciding to retain personal information that is unsolicited, agencies should consider the purpose for which they intend to hold that information.

Information that is not collected from the individual concerned

3.23 We asked in the issues paper whether the notification requirements of principle 3 should apply even when information has not been collected from the individual concerned (because one of the exceptions to principle 2 applies). Such a change would bring New Zealand's Privacy Act into line with legislation in some other jurisdictions such as Australia, where the National Privacy Principles in the Privacy Act 1988 (Cth) require notice to be given regardless of whether personal information is obtained from the individual concerned or from someone else.[103]

3.24 Submitters were evenly divided on this question. Arguments in favour of the change were that:

- it would promote openness and transparency;
- agencies would only have to take such steps as are reasonable in the circumstances to comply with principle 3; and
- the exceptions to principle 3 would continue to apply.

The following arguments against the suggested amendment were made in submissions:

- There is no identified problem at present, and any problems in particular sectors could be dealt with through codes of practice.
- The benefits of the change do not warrant the compliance costs that would be involved.
- Individual notification would be impracticable in many instances.
- A requirement to notify people in cases where information is being collected from a third party could actually lead to privacy breaches, as notification that particular information has been collected might go to the wrong person.

3.25 Requiring notification to the individual concerned where information is collected from a third party would be a very significant change to the collection principles, and would therefore need a significant level of support to go ahead. Given that opinion was divided on this issue, and that some significant objections to the change were put forward (including by OPC), we recommend no change.

103 Privacy Act 1988 (Cth), sch 3, National Privacy Principle 1.5. See also *For Your Information* at 779–783; Australian Government "Australian Privacy Principles: Exposure Draft" (2010) principle 6.

A new health and safety exception

3.26 At present, principles 2 and 3 do not have "health and safety" exceptions, equivalent to the exceptions to principles 10 and 11, although there is an exception to rule 2 of the Health Information Privacy Code (HIPC) which allows for collection of information other than from the individual concerned where collection from that individual would "prejudice the safety of any individual".[104] We proposed in the issues paper that a health and safety exception should be added to principle 2, and perhaps to principle 3.

3.27 Almost all submitters who responded to this proposal supported it. Some submitters thought it would be particularly useful in the mental health field, although in general situations involving mental health issues will be covered by the HIPC rather than the Act itself. However, OPC was opposed to the proposal in relation to principle 3, and with regard to principle 2 OPC felt that a compelling case for the amendment had not been made out in the issues paper. In OPC's view, the kinds of collections to which a health and safety exception might be relevant can probably already be undertaken using one of the generic exceptions to principle 2, particularly the "no prejudice", "prejudice the purposes of collection" and "not practicable" exceptions.

3.28 We agree with OPC that it would not be appropriate to add a health and safety exception to principle 3. If personal information is collected from the individual concerned, that individual has a right to know the purpose of collection, where the information is going, and the other matters covered by principle 3. If a health and safety exception were to be added to principle 3, there is a danger that agencies would avoid taking reasonable steps to provide such information when dealing with individuals with mental illness or with physical or mental disabilities.

3.29 We do, however, think that a health and safety exception should be added to principle 2. It is likely that there will be situations in which health or safety considerations mean that it is not possible to collect information from the individual concerned. An employer dealing with a workplace accident might, for example, need to get information about an injured worker from a family member; or a social worker might need to collect information from a third party in a case where a child appears to be at risk of harm. We acknowledge OPC's point that existing exceptions can probably cover such situations, but we still think that agencies will find it helpful to have a specific exception (just as there is already a specific exception covering maintenance of the law).

3.30 The new exception to principle 2 should apply where an agency has reasonable grounds for believing that a "serious" threat to health or safety exists. We recommend at R31 below that the Act should set out criteria for assessing seriousness for the purposes of health and safety exceptions to principles 2, 6, 10 and 11.

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

RECOMMENDATION

R12 Principle 2(2) should be amended by adding a new exception covering situations in which an agency believes, on reasonable grounds, that non-compliance is necessary to prevent or lessen a serious threat to the health or safety of any individual.

"No prejudice" and "not reasonably practicable" exceptions

3.31 Both principle 2 and principle 3 include exceptions for situations in which the agency has a reasonable belief "that non-compliance would not prejudice the interests of the individual concerned" or "that compliance is not reasonably practicable in the circumstances of the particular case".[105] We proposed in the issues paper that the "no prejudice" exception should be deleted. We argued that the agency collecting the personal information may not be in a position to determine whether or not the individual's interests will be prejudiced, and that a focus on prejudice to the interests of individuals ignores the cumulative effect of collections which may each be relatively harmless but which, taken together, may have negative consequences.[106] With regard to the "not reasonably practicable" exception, we asked whether it needed to be made clear that the exception should not be relied on where an agency wishes not to comply with principle 2 simply because the individual concerned refuses to provide the information, or because the agency believes that the individual would refuse.[107]

3.32 There was no consensus in submissions with regard to the "no prejudice" exception. Submitters who supported our proposal to delete the exception said that it is not always apparent to agencies what is or is not in the interests of individuals, and that the exception involves a subjective judgement on the part of agencies. Those who opposed the proposal argued that the "no prejudice" exception was an important part of the Act's balance between the privacy rights of individuals and the operational needs of agencies, and that the proposal could impose compliance costs on agencies while providing only limited benefits to individuals.

3.33 With regard to the "not reasonably practicable" exception, a number of submitters supported the suggested clarification. OPC commented that it would seem self-evident that the exception cannot be relied on in situations that involve unwillingness to give consent, but that it could be useful to make this absolutely clear. IHC agreed that the exception should not be used simply because an agency is unable to get consent to collection. In addition, IHC said that the exception should not be used when an agency wishes to avoid collecting information from an individual with an intellectual disability simply because it might take longer to explain matters to that individual or for the individual to understand, consider and respond to a request for information. A few submitters opposed the suggested change, and one government agency argued that principle 2 does not give individuals a right of veto over the collection of their information.

105 Privacy Act 1993, s 6, principles 2(2)(c) and (f), 3(4)(b) and (e).

106 Issues Paper at 92–93.

107 Ibid, at 93.

3.34 We recommend that there should be no change to these two exceptions. There was a significant amount of opposition to our proposal to delete the "no prejudice" exception, and we note that OPC thought, on balance, that the exception should be retained. While we continue to believe that agencies will often not be in a position to assess the potential prejudice to an individual, we point out that an agency can only rely on the exception if it has *reasonable grounds* to believe that its actions will not prejudice the individual's interests, and that the onus of proof that the exception applies will lie with the agency if a complaint is made about its actions.[108]

3.35 The "not reasonably practicable" exception applies to situations in which information cannot be collected from the individual concerned, or the individual concerned cannot be notified in accordance with principle 3. In our view, it is intended to apply in such circumstances as where it is impossible, or unreasonably difficult, to contact the individual; the individual is in a coma; or the information the agency is seeking is the opinion of a third party (such as a doctor) about the individual.[109] We agree with IHC that the exception should not be relied on because an agency finds it inconvenient or too time-consuming to collect information from an individual with an intellectual or physical disability. Nor should it be relied on simply because an individual refuses to provide information to an agency, or because the agency believes that the individual would refuse. There will often be situations in which no exception to the principle applies and therefore information can only be collected in compliance with the Act if it is collected from, or with the consent of, the individual concerned. In such cases we think it would be a clear breach of the Act for an agency, having failed to obtain the information from the individual, to claim that compliance with principle 2 is "not reasonably practicable". We do not think any amendment to the principle can usefully provide further clarification of this point.

Authorisation and statistical or research exceptions to principle 3

3.36 Following a recommendation of the Privacy Commissioner, we proposed in the issues paper that two exceptions to principle 3 should be deleted.[110] These exceptions are principle 3(4)(a), which allows an agency not to comply with principle 3 if non-compliance is authorised by the individual concerned; and principle 3(4)(f)(ii), which provides for non-compliance 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 concerned".

3.37 The Privacy Commissioner's arguments for deleting principle 3(4)(a) were that:

- This provision could be seen as allowing organisations to seek 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.

108 Privacy Act 1993, s 87.

109 The latter example might also be covered by the exception that applies where "compliance would prejudice the purposes of the collection": principles 2(2)(e) and 3(4)(d).

110 Issues Paper at 94–95; *Necessary and Desirable* at 67–70 (recommendations 20 and 21).

- 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.

3.38 More submitters supported than opposed the proposal to delete the authorisation exception, but no new arguments were put forward in support. Arguments against the proposal were that:

- No examples of abuse of the exception have been identified.
- The exception is useful, and individuals should be able to choose to waive their rights under principle 3.
- The exception has practical uses in everyday situations where an implied waiver is understood by both parties, such as when a car is dropped off to the mechanic and the mechanic takes the customer's phone number in order to contact the customer. Wholesale deletion of the exception may not be the best way of dealing with the concerns that were identified in the issues paper.

3.39 We remain convinced by the arguments originally put forward by the Privacy Commissioner, and we recommend that principle 3(4)(a) be deleted. We do not think that the deletion will prove problematic in everyday situations in which there is no expectation that an agency will go through all of the matters set out in principle 3(1). We think that these situations are adequately dealt with by the fact that agencies are required to take only such steps as are, in the circumstances, reasonable, together with exceptions such as "no prejudice" or "not reasonably practicable".

3.40 In relation to principle 3(4)(f)(ii), the Privacy Commissioner argued that:

- 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.
- 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.

Most submitters who commented on the proposed deletion of principle 3(4)(f)(ii) supported the proposal, but gave no reasons for their support. A few agencies opposed the proposal, arguing that the exception is relied on for research that has high public benefit and does not prejudice individual privacy, and that exception (f)(ii) is little different from (f)(i), which is not proposed for deletion.

3.41 We recommend that principle 3(4)(f)(ii) be deleted, for the reasons put forward by the Privacy Commissioner. The statistical and research exceptions to principles 2, 10 and 11 are important, and should be retained. We also recommend below that there should be a new statistical and research exception to principle 12. However, we do not think that such an exception to principle 3 is justified. Generally speaking, ethical standards for research require that research subjects are aware of the fact that personal information is being collected from them, the purpose for which it is collected, and so on.[111]

111 See, for example, Health Research Council *Guidelines on Ethics in Medical Research* (2002, revised 2005) at 38; Market Research Society of New Zealand *Code of Practice* (revised 2008) especially arts 4 and 7(b).

Such ethical standards are closely related to requirements for research subjects to give informed consent to participation in research.[112] This widely-accepted ethical position will be supported by the deletion of exception (f)(ii) to principle 3.

3.42 Nonetheless, there will be cases in which, for quite legitimate reasons, information is collected from the individual concerned but the individual is not informed at the time of collection of the matters required by principle 3.[113] Even without principle 3(4)(f)(ii), such "non-disclosing" collections may be permissible under the Act because:

- the information collected is not "personal information" (because it is not "about an identifiable individual");[114]
- non-notification will not prejudice the individual's interests;[115]
- notification would prejudice the purposes of the collection;[116]
- notification is not reasonably practicable in the circumstances;[117]
- the information will not be used in a form in which the individual is identified;[118] or
- non-compliance with principle 3 is authorised or required under law.[119]

We note that Statistics New Zealand was not opposed to the proposed deletion, since they could rely on the "prejudice the purposes of collection" exception instead. Furthermore, where it is not practicable to disclose the matters set out in principle 3 at the time of collection, the Act provides that disclosure may take place "as soon as practicable after the information is collected".[120] This may be relevant in some research contexts, where the subjects cannot be told the purpose of the research at the time of collection, because such knowledge might influence the results, but can be told shortly afterwards.

3.43 We do not think there is any inconsistency in deleting exception (f)(ii) but leaving (f)(i). Exception (f)(i) allows non-compliance with principle 3 where the information "will not be used in a form in which the individual concerned is identified". Exception (f)(ii), by contrast, refers to information that 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". Thus, (f)(i) deals with "use" while (f)(ii) deals with publication. Exception (f)(ii) would appear to allow non-transparent statistical and research uses so long as any resulting publication does not make the research subjects identifiable; exception (f)(i) will only apply if the use itself involves information that has been de-identified.

---

112 See PDG Skegg "Consent and Information Disclosure" in John Dawson and Nicola Peart (eds) *The Law of Research: A Guide* (University of Otago Press, Dunedin, 2003) 233.

113 See Selene Mize "Non-Disclosing and Deceptive Research Designs" in John Dawson and Nicola Peart (eds) *The Law of Research: A Guide* (University of Otago Press, Dunedin, 2003) 253.

114 See discussion of the definition of "personal information" in ch 2.

115 Privacy Act 1993, s 6, principle 3(4)(b).

116 Privacy Act 1993, s 6, principle 3(4)(d).

117 Privacy Act 1993, s 6, principle 3(4)(e).

118 Privacy Act 1993, s 6, principle 3(4)(f)(i).

119 Privacy Act 1993, s 7(4).

120 Privacy Act 1993, s 6, principle 3(2).

RECOMMENDATION

R13 Principles 3(4)(a) and 3(4)(f)(ii) should be deleted.

Principle 4 – manner of collection

3.44 Principle 4 is, for the most part, unproblematic. However, there is some uncertainty about its application to attempts to collect personal information, where no information is in fact collected.[121] We proposed in the issues paper that principle 4 should be amended to make it clear that it applies to attempts to collect information.[122] We saw this proposal as being particularly useful in providing a remedy in cases of attempted surveillance, where surveillance equipment has been installed with the intention of collecting information about an individual. If the surveillance equipment has been installed in such a way that it is unlawful, unfair or potentially unreasonably intrusive, the fact that no personal information is in fact collected should not preclude the affected individual from bringing a complaint under the Act. Examples of attempted surveillance in which no personal information is collected could include situations in which the equipment fails to work properly, or where the information collected does not fall within the definition of "personal information" (perhaps because the individual in question is not identifiable from the recorded material). In such a situation, the individual could still suffer stress, humiliation or loss of dignity as a result of knowing that he or she had been under surveillance.

3.45 Most submitters on this question supported our proposed amendment. The New Zealand Law Society commented that principle 4 is directed at the conduct of agencies, so it should apply whether or not information is actually collected. OPC saw the proposal as having some promise, although it also considered that there was a danger that the law might over-reach the problem and create new difficulties. In addition, OPC noted that there will be some situations in which, faced with objectionable attempts to collect their personal information, individuals will refuse to provide the requested information. An example of such a situation is a survey which asks questions about very personal matters.

3.46 We recommend that principle 4 should be amended so that it is clear that it applies to attempts to collect personal information, regardless of whether or not those attempts are successful. We do not think that this amendment would open the door so wide that the principle would cover attempts at collection where the individual is realistically able to refuse to provide the information, even if provision of the information would intrude significantly on the individual's personal affairs. For example, if a marketing company asks very intrusive questions on a survey form, but there is no compulsion on an individual to complete the form, this would not be unfair or unreasonably intrusive. However, intrusive questions asked as part of a job interview, when an individual might feel under pressure to answer, *could* perhaps be covered by principle 4, even if the individual refused to answer them. We also note that, in a case of unsuccessful

121 This issue has been discussed by the Human Rights Review Tribunal, but it has not yet been required to decide the matter: *Stevenson v Hastings District Council* [2006] NZHRRT 7 at [64]–[72]; *Lehmann v CanWest Radioworks Limited* [2006] NZHRRT 35 at [67]–[68].

122 Issues Paper at 95–96.

attempted collection, it will be possible to take into account the fact that no information was collected in assessing harm for the purposes of any complaint about that collection. The level of harm will generally be less if no personal information was collected, and this can be reflected in the type of remedies negotiated or awarded.

RECOMMENDATION

R14 Principle 4 should be amended to make it clear that it applies to attempts to collect information.

SECURITY, ACCURACY AND RETENTION PRINCIPLES

3.47 Principles 5, 8 and 9 are only loosely related, but all involve the safe and fair handling of information which an agency "holds". Principle 5 requires agencies to hold information securely, so that it is protected against loss or misuse; principle 8 states that agencies shall not use personal information that they hold without taking such steps as are reasonable to ensure that the information is accurate, up to date, complete, relevant and not misleading; and principle 9 provides that an agency that holds personal information shall keep that information for no longer than is required for the purposes for which the information may lawfully be used.

Principle 5 – security

3.48 We suggested in the issues paper that there appeared to be a gap in principle 5 in relation to the issue of employee "browsing". This term is used to describe cases of access to personal information that an agency holds by employees who are authorised to access the information, but who do so for an unauthorised purpose. For example, an employee who has access to hospital medical records might access records relating to a celebrity purely out of curiosity, or in order to pass information on to the media. We commented that the current wording of principle 5 is not absolutely clear with respect to browsing, and noted that any gap in the coverage of principle 5 is further accentuated by the fact that section 252(2) of the Crimes Act 1961 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 proposed that the principle should be amended to make it 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 do not access, use, modify or disclose that information for other purposes.[123]

3.49 There was no disagreement in submissions with the principle that agencies should, as a matter of good practice, act to prevent employee browsing. The point was made that many agencies already have policies in place to prevent such browsing, and treat it as part of their obligations under principle 5. Most submitters agreed with our proposal to amend the principle to make it absolutely clear that it covers employee browsing, but some thought that such an amendment was unnecessary or undesirable. One submitter said that, instead of amending

123 Ibid, at 96–97.

principle 5, a new provision should be added elsewhere in the Act making employee browsing a breach of the Act, while another said that if there is a need to do more to address employee browsing it should be done through civil or criminal liability rather than an amendment to the Privacy Act. There was also support from one submitter for amending section 252 of the Crimes Act so that browsing incidents would be covered by the offence of unauthorised access to a computer system. A few submitters were concerned about the possibility that compliance with principle 5 might come to require the introduction of expensive and cumbersome systems to track all employee access to data.

3.50 We were reassured by the general belief among submitters that principle 5 already requires agencies to take steps to prevent employees from accessing personal information for purposes other than those for which the information is held, and that this is also a matter of good practice. As a result, we have concluded that an amendment to principle 5 is not required. While the current wording of principle 5 is not absolutely clear with respect to browsing, we think that the intent of the provision is quite clear: an agency must take reasonable steps to ensure not only that access to personal information held by the agency is limited to employees who are authorised to do so, but also that employees are accessing such information only for authorised purposes. Rather than adding to the length of principle 5 by putting this matter beyond doubt, we now favour dealing with the matter through guidance from the Privacy Commissioner. We recommend that the Privacy Commissioner should issue guidance material making clear that employee browsing is a breach of principle 5, and setting out the kinds of steps agencies should take to protect against employee browsing.

3.51 With respect to section 252(2) of the Crimes Act, we suggest that this could be reviewed as part of a wider review of the adequacy of the law to deal with covert data surveillance. We recommended that such a review should take place in our report for stage 3 of this Review.[124]

RECOMMENDATION

R15 The Privacy Commissioner should develop guidance material with respect to principle 5 and the issue of employee "browsing" of personal information.

Principle 8 – data quality

3.52 We noted in the issues paper that principle 8 refers to checking the accuracy of information before "use", and does not expressly refer to disclosure. "Use" in principle 8 should probably already be interpreted as including disclosure,[125] but it is arguable that, since the Act has separate use and disclosure principles, "use" in principle 8 has the same meaning as in principle 10. We proposed, in line with an earlier recommendation of the Privacy Commissioner,[126] to provide greater clarity by amending principle 8 to read "shall not use or disclose".

124 Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, 2010) at 25–27.

125 See *Herron v Speirs Group Ltd* [2006] NZHRRT 12 at [52]–[54]; *EFG v Commissioner of Police* [2006] NZHRRT 48 at [69]–[75].

126 *Necessary and Desirable* at 79–80 (recommendation 26).

3.53 There was more support for than opposition to this proposal. However, there was a significant level of opposition, which appeared to result largely from a misapprehension about what the Commission was proposing. A number of agencies were concerned that the Commission proposed to introduce more rigorous requirements for checking data quality than currently exist. In fact, the only change proposed by the Commission was an amendment to clarify that principle 8 applies to disclosure as well as use. Agencies would still be required only to take "such steps (if any) as are, in the circumstances, reasonable …, having regard to the purpose for which the information is proposed to be used [or disclosed]", to check data quality before use or disclosure. The wording of the principle clearly anticipates that, in some circumstances, an agency will not need to take any steps to check data quality. Principle 8 will also be overridden by disclosure that is authorised or required under other legislation, provided that such legislation is appropriately worded. In particular, a disclosure of personal information under the Official Information Act 1982 (OIA) will not have to meet the requirements of principle 8. We recommend that principle 8 should be amended as proposed in the issues paper.

RECOMMENDATION

R16 Principle 8 should be amended so that it clearly applies to both use and disclosure.

Principle 9 – retention

3.54 Principle 9 states that personal information shall not be kept "for longer than is required for the purposes for which the information may lawfully be used", rather than for the purposes for which it was *collected*. In the issues paper we noted that the phrase "the purposes for which the information may lawfully be used" can be interpreted very broadly. As a result, it had been suggested to us that principle 9 was almost meaningless, since there is always some purpose for which information may lawfully be used, even though that purpose may be quite unrelated to the purpose for which the information was originally obtained. However, our view was that principle 9 does serve a useful purpose, and that its wording should not be changed.[127] The existence of principle 9 prompts agencies to think about whether they need to retain personal information, and the principle can also be given greater specificity in codes of practice (as is the case in the Credit Reporting Privacy Code, for example). We also noted that the words "may lawfully be used" could be interpreted as including the restrictions on use in principle 10. This would mean that personal information cannot be retained with a view to using it for a purpose other than that for which it was obtained, unless one of the exceptions to principle 10 applies.

3.55 There was very little disagreement in submissions with our view that principle 9 should remain unchanged. Both OPC and Professor Paul Roth commented that it is a relatively weak principle, but had no suggestions for improving it. OPC emphasised the importance for privacy protection of controls on retention, particularly as technological developments have made it much easier to store

127 Issues Paper at 98–99.

vast quantities of data for very long periods of time. We agree that principle 9 is an important principle, despite being relatively brief and somewhat broadly worded, and believe it should remain in its current form.

3.56 The issues paper also asked whether principle 9 should specify how information should be disposed of once an agency decides that it will no longer be retained, or whether guidance from OPC on disposal would be helpful. We did not think it would be helpful for the principle to deal with methods of disposal, and most submitters agreed. A number of submitters said that guidance from OPC would be helpful, but we did not get the impression that this is an issue where agencies are having particular difficulties, so we do not see such guidance as a priority.

3.57 Some agencies sought greater clarity about the relationship between principle 9 and the Public Records Act 2005. We deal with this issue in chapter 8.

ACCESS AND CORRECTION PRINCIPLES

3.58 Principle 6 states that individuals have 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. A range of exceptions to principle 6 (that is, grounds on which agencies may refuse to provide access to personal information) are set out in Part 4 of the Act. Procedural matters relating to rights of both access and correction are contained in Part 5 of the Act. We discuss the provisions of Parts 4 and 5 here. In addition, section 55 of the Act provides that principles 6 and 7 do not apply in respect of certain types of information. We recommend one addition to section 55 in chapter 4.

"Coerced access"

3.59 We are not aware of any problems with the wording of principle 6, but we did raise one issue about the application of this principle in the issues paper. Concerns have been raised about "coerced access requests", in which a third party requires an individual to use his or her access rights under principle 6 to obtain that individual's personal records, so that the individual can pass those records on to the third party. For example, employers might require current or prospective employees to access their criminal records and give them to their employers; or insurance companies might require individuals seeking to take out insurance to access and pass on their medical records.[128] The Data Protection Act 1998 (UK) contains provisions that prohibit employers, prospective employers and service providers from requiring individuals to produce certain types of (mainly criminal) records obtained by exercising their access rights; and that void any term or condition of a contract that purports to require an

128 See discussion in *Necessary and Desirable* at 363–367 and *4th Supplement to Necessary and Desirable* at 31; Roth *Privacy Law*, above n 99, at [PVA6.9(f)]. A recent article about criminal records checking, particularly in the employment context, concludes that privacy laws "do not lend themselves" to protecting the different interests involved, and that consideration should be given instead to the introduction of specific legal restrictions on the disclosure of criminal records information by official record-keepers. See Moira Paterson "Criminal Records, Spent Convictions and Privacy: A Trans-Tasman Comparison" [2011] NZ L Rev 69 at 87–89

individual to produce health records obtained by using their access rights.[129] The Privacy Commissioner has recommended the introduction of similar controls in the Privacy Act here.[130]

3.60 Although the question in the issues paper related to coerced access requests, a number of submitters pointed out that coerced authorised disclosures are equally problematic, and are probably more common. A coerced authorised disclosure is a disclosure of personal information by an agency that has purportedly been authorised by the individual concerned, in accordance with principle 11(d), but where the individual's authorisation has not been freely given. For convenience, we discuss both coerced access requests and coerced authorised disclosures here, and refer to the issue generically as "coerced access".

3.61 There was no clear pattern in the submissions on coerced access, but a number of submitters agreed that there was a problem. The New Zealand Law Society said that coerced access is a significant problem in relation to access to health information by employers and insurance companies, but thought that the issue required wider scrutiny than is possible within the present review. An individual lawyer suggested that coerced access involving insurance companies and health information is an issue for the Health Information Privacy Code rather than the Act itself. The New Zealand Council of Trade Unions (CTU) endorsed the view that coerced access is a problem in the employment field, and referred specifically to injured workers feeling compelled to sign consent forms that allow their medical information to be disclosed to their employers. In the CTU's view, workers often lack a full understanding of the purpose of such authorised disclosures. OPC said that coerced access remains a problem that should be addressed, and that it is especially problematic where there is a power imbalance, or where a universal industry practice exists, so that individual choice is not an effective means of responding to pressure. OPC noted that some of the issues concerning coerced release of criminal records had been dealt with indirectly through the Criminal Records (Clean Slate) Act 2004, although OPC continues to hold concerns in this area. OPC also noted its inquiry into insurance company practices of requiring access to medical records.[131] A different type of coercion was raised with us by the Police, who referred to instances in which a dominant abusive partner has coerced another adult or a child into making an access request to Police. The Police said that there is currently no mechanism in the Act for ensuring that access requests are freely made, and suggested that section 45 could be amended so that agencies can refuse access requests if they have evidence that they are coerced.

3.62 Coerced access is a complex issue, involving a range of types and degrees of coercion, and we do not see any easy solutions to it. We begin with the most serious types of coercion, those raised with us by the Police. We agree with the Police that section 45 should be amended to deal with access requests that are made under direct threat of physical or mental harm, as in situations of abusive domestic relationships. Section 45 currently requires, in the case of access requests, that agencies satisfy themselves concerning the identity of the individual making the request; adopt procedures to ensure that the requested

129 Data Protection Act 1998 (UK), ss 56–57.

130 *Necessary and Desirable* at 363–367 (recommendations 151 and 152).

131 Privacy Commissioner *Collection of Medical Notes by Insurers: Inquiry by the Privacy Commissioner* (June 2009).

information is received only by the individual or his or her agent; and ensure that, where a request is made by an individual's agent, the agent is properly authorised by the individual to obtain the information. We recommend that section 45 be amended to provide that an agency shall not give access to information requested under principle 6 if the agency has reasonable grounds for believing that the individual concerned is making the request under duress in the form of actual or threatened physical harm or psychological abuse. Section 45 already plays an important role in ensuring that third parties do not misuse principle 6 to obtain personal information that is not theirs, and we believe that our recommendation will strengthen this protection.

3.63 We also note that failure by agencies to comply with section 45 is not currently a clear ground for a complaint under the Act. We recommend that section 66(2) should be amended to refer expressly to a failure by an agency to comply with the requirements of section 45 as being an interference with privacy. Such an amendment will give agencies a greater incentive to ensure that they take the precautionary steps required by section 45.

3.64 A parallel provision is needed to deal with cases of authorised disclosure where the authorisation is obtained under severe duress. We recommend that a new definition of "authorise" should be added in section 2 of the Act. The effect of the definition should be to exclude from the meaning of "authorise" situations in which an individual's agreement is obtained under duress in the form of actual or threatened physical harm or psychological abuse. We note that this definition would be a negative one: it would define "authorise" in terms of what it is *not*. We have considered the option of defining "authorise" in positive terms; that is, defining what it *is*. However, we think authorisation is a complex matter, and one that cannot readily be pinned down in a statutory definition. We are concerned that defining "authorise" in positive terms might create more difficulties than it solves, and so we do not recommend it.

3.65 We have given careful thought to whether the Act can be amended to deal with less extreme forms of coercion, such as those that are economic in nature, but we have been unable to find a workable solution to this problem. We have no doubt that some cases of coerced access are an abuse of individuals' rights under the Act, and that individuals may make access requests or provide authorisation only reluctantly in order to provide their personal information to some third party, in the context of a power imbalance between the individual and that third party. However, we do not think that an amendment to the Act can readily solve this problem. At the same time, we note that reform in other areas may help to deal with coerced access:

- As some submitters noted, the Criminal Records (Clean Slate) Act 2004 has dealt with concerns about criminal records with respect to individuals covered by the clean slate scheme. It is an offence under section 18 of that Act to require or request that an individual disregard the effects of the clean slate scheme and disclose, or give consent to the disclosure of, his or her criminal record.
- Some of the concerns about medical records may be able to be addressed in the Health Information Privacy Code, which we are not reviewing in this report. However, the Code applies only to the handling of health information

by health agencies (which include agencies providing health, disability, accident or medical insurance, and accredited employers under the Injury Prevention, Rehabilitation, and Compensation Act 2001).[132]

RECOMMENDATION

R17 Section 45 should be amended to provide that an agency shall not give access to information requested under principle 6(1)(b) if the agency has reasonable grounds for believing that the individual concerned is making the request under duress in the form of actual or threatened physical harm or psychological abuse.

RECOMMENDATION

R18 Section 66(2) should be amended to provide clearly that failure by an agency to comply with the requirements of section 45 is an interference with privacy.

RECOMMENDATION

R19 "Authorise" should be defined in section 2 as excluding situations in which an individual's agreement is obtained under duress in the form of actual or threatened physical harm or psychological abuse.

Statement of correction sought but not made

3.66 We supported in the issues paper a recommendation of the Privacy Commissioner[133] which would require agencies to inform requesters, in cases where an agency is not willing to correct an individual's personal information, of their right to request that a statement be attached to the information of the correction sought but not made. The Tribunal has held that no such obligation exists in the Act at present.[134] There was general support for this proposal in submissions, but some submitters noted that there can be practical difficulties with attaching a statement. Where information is held in electronic form, submitters noted, it is not always possible to add comments to the relevant field, particularly in the case of old databases. On the other hand, it was said that if a notation is attached to a paper-based file, it may not be possible to include the notation if the information is later disclosed electronically (including through information matching programmes). One submitter suggested that, where it is not practicable to attach a statement to the information concerned, informing requesters of their right to ask for such a statement to be attached would only lead to frustration. Some submitters were also concerned to ensure that, where a statement of the correction sought is attached at an individual's request, the agency should be free to add a commentary as to why it disagrees with the statement.

3.67 We recommend that principle 7 be amended as proposed in the issues paper. We note that agencies are required only to "take such steps (if any) as are reasonable in the circumstances" to attach to the information a statement of the correction sought but

132 Health Information Privacy Code 1994, cl 4(2)(i) and (j).

133 *Necessary and Desirable* at 76 (recommendation 24).

134 *Plumtree v Attorney-General* [2002] NZHRRT 10 at [137]–[138], [145].

not made. There is nothing in principle 7 preventing agencies from also attaching a comment about why they disagree with this statement. We acknowledge that, where it is not practicable for the agency to attach a statement, informing the individual of his or her right to such an attachment would be meaningless, and we think that this point can be accommodated in the drafting of the amendment to principle 7.

RECOMMENDATION

R20 Where an agency is not willing to correct personal information in response to a request made under principle 7, the agency 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.

Part 4 of the Act – good reasons for refusing access

3.68 The reasons for refusing access to personal information, set out in Part 4 of the Act, are based on the withholding grounds under the OIA. It may be desirable to maintain some consistency between the grounds for withholding access to information under the two Acts, although there will be grounds that are appropriate for one Act but will not be relevant for the other. The Law Commission is also currently reviewing the OIA, so we can take this issue of consistency between the two Acts into account in that review. Law enforcement grounds for refusing access are discussed in chapter 9.

Threshold for applying access refusal grounds

3.69 Trade Me's submission raised a concern about the difference between the thresholds for the maintenance of the law ground for refusing access and the equivalent exception for disclosing information under principle 11. The various access refusal grounds in section 27 can be applied where the relevant prejudice or danger "would be likely". On the other hand, the use and disclosure exceptions to principles 10 and 11 come into play when the agency "believes, on reasonable grounds" that one of the exceptions applies. The "would be likely" test focuses on the degree of perceived risk, while "believes, on reasonable grounds" centres on the evidential basis for the agency's perception. Trade Me submitted that the "belief on reasonable grounds" threshold would be a more suitable one for agencies to apply when relying on the maintenance of the law access refusal ground.

3.70 We have considered Professor Paul Roth's analysis of the phrase "would be likely" as used in section 27.[135] The High Court has interpreted the phrase as meaning "a distinct or significant possibility", and has stated that in order to rely on one of the section 27 grounds for withholding information, "an agency must show there is a real and substantial risk to the interest being protected".[136] A later Privacy Commissioner case note records the Privacy Commissioner's

135 Roth *Privacy Law*, above n 99, at [PVA27.5].

136 *Nicholl v Chief Executive of Work and Income* HC Rotorua, AP 255/01, 6 June 2003, at [13].

view that "likely" in section 27 "means only that there must be a real risk of something occurring". The agency that wishes to withhold information "has to provide sufficient evidence to indicate that a danger in fact exists".[137]

3.71 As the phrase has been interpreted, there may not be a significant difference in effect between the threshold for the access refusal grounds in section 27 and the threshold for the exceptions in principles 10 and 11.[138] In each case, the agency will need to have some reasonable evidential basis on which to base its conclusion that there is a risk of prejudice to the interest in question. Nonetheless, having different formulations can be confusing and can imply that there is a difference in their application. We agree that it is desirable to have a uniform test and that section 27 should be amended to include the agency "belief on reasonable grounds" threshold that is used in principles 10 and 11. We recommend that this be addressed in redrafting. Although Trade Me's submission was concerned with the maintenance of the law access refusal ground, there needs to be consistency across all of the grounds for refusing access. We therefore recommend that "believes, on reasonable grounds" should apply as a threshold to all of the refusal grounds included in sections 27, 28 and 29. This would be in addition to the test of "would" or "would be likely" (as the case may be) in the access refusal grounds in those sections.

RECOMMENDATION

R21 Sections 27 to 29 should be amended to incorporate the agency "belief on reasonable grounds" threshold, for consistency with principles 10 and 11.

Safety

3.72 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". It has been held that this provision relates only to physical safety, not to health or "mental safety".[139] We asked whether this section should be expanded to include other elements, such as requiring a serious threat, referring to health, and including threats to *public* health and safety. Such changes would bring the ground more into line with the health and safety exceptions to principles 10 and 11. We noted that, while health reasons for refusing access are also covered by section 29(1)(c), that section applies only to situations in which information needs to be withheld to protect the physical or mental health of the individual making the request.

3.73 Most submitters who commented on this issue supported some expansion of the current safety ground. A number of submitters supported aligning section 27(1)(d) with the wording of the health and safety exceptions to principle 10 and 11, while a few said that the section should refer to health and to mental safety or mental health. However, OPC favoured leaving section 27(1)(d) unamended. They submitted that elements of the health and safety exceptions to the use and disclosure principles that are not present in section 27(1)(d) are of limited

137 *Information About Student Withheld Because of Fears of Safety* [2007] NZ PrivCmr 19, Case Note 92314.

138 Principles 2 and 3 also have a "believes, on reasonable grounds" test for their exceptions.

139 *O v N* Complaints Review Tribunal 4/96, 12 March 1996 at [15].

relevance to access requests. They saw the proposed ground for refusal relating to harassment (discussed below) as a better way of dealing with perceived gaps in the safety ground.

3.74 We recommend that section 27(1)(d) should be amended so that an agency may refuse to disclose information requested under principle 6 if disclosure of that information would be likely to present a serious threat to public health or public safety, or to the life or health of any individual. It will be apparent that this wording is based on that of the health and safety exceptions to principles 10 and 11. We do not think it is necessary to refer expressly to mental health or mental safety. With regard to the seriousness element, the Ombudsmen questioned whether this was needed, since the Tribunal and the courts have imported a seriousness test into the phrase "would be likely".[140] While acknowledging this point, we think that "would be likely" must relate primarily to seriousness in the sense of the probability of a threat, and perhaps also to the threat's imminence. It does not necessarily cover the consequences if the threat were to eventuate. We tease out these elements of seriousness in our discussion of the health and safety exceptions to principles 10 and 11 below, and recommend at R31 that the Act should set out criteria for assessing seriousness for the purposes of health and safety exceptions to principles 2, 6, 10 and 11.

3.75 We accept that a broader health and safety exception of the kind we recommend here is more relevant to the disclosure principle, and perhaps also to the OIA,[141] than to access by individuals to their personal information. Nonetheless, we think there could be occasions when agencies, in response to access requests, need to withhold personal information for reasons relating to the health of individuals that are not covered by section 29(1)(c), or for reasons of public health or safety. The amendment we have recommended would also bring section 27(1)(d) into closer alignment with the equivalent provisions, both current and proposed, in the Privacy Act 1988 (Cth).[142] While there could be a concern that the widening of this ground will lead to access being refused more often, we emphasise that agencies will need good reasons for believing that a threat to health or safety is both "likely" and "serious". These requirements should act as a check on overuse of this ground for refusal by agencies.

RECOMMENDATION

R22 Section 27(1)(d) should be amended so that an agency may refuse access if disclosure of the information would be likely to present a serious threat to public health or public safety, or to the life or health of any individual.

140 See the discussion of "would be likely" in Roth *Privacy Law*, above n 99, at [PVA27.5].

141 Relevant withholding grounds under the OIA are found in Official Information Act 1982, ss 6(d), 9(2)(c).

142 Privacy Act 1988 (Cth), sch 3, principle 6.1(a) and (b); *For Your Information* at 986–987; Australian Government "Australian Privacy Principles: Exposure Draft" (2010) principle 13(3)(a).

Harassment

3.76 Related to the expansion of the safety ground is the question of whether the Privacy Act should provide for a specific ground for refusal of access in cases where providing information is likely to lead to harassment of third parties. This issue can arise in requests involving mixed information about the requester and others. For example, a requester who has a grievance about his or her medical treatment might request the names of all of those involved in providing that treatment. In some cases, individuals may use such information to make repeated, unwanted contact with other individuals in ways that fall short of posing a physical danger to those individuals but that seriously detract from their quality of life. The question is whether existing grounds for refusal are adequate to deal with such cases. Possible grounds for refusal include the safety ground,[143] and the ground relating to "unwarranted disclosure of the affairs of another individual".[144]

3.77 There was a reasonable level of support in submissions for adding a ground for refusal of access relating to harassment. A number of submitters, however, raised the issue of how harassment would be defined, or the threshold of seriousness that would be required for a threat of harassment to be established.

3.78 We consider that existing grounds do not clearly cover risk of harassment, and that a new harassment ground should be added to section 29. The safety and "unwarranted disclosure of the affairs of another individual" grounds can be used to cover threat of harassment, but this involves something of a stretch. Harassment often does not involve any threat to physical safety, although if the safety ground is expanded as we have recommended above it is possible that harassment could be seen as endangering mental health. Likewise, where likelihood of harassment is the issue, the problem is not really that release of personal information might disclose "the affairs of another individual" but rather that it might lead the requester to harass that individual. We think it is best to have a specific ground for refusal dealing with harassment. We do not think that harassment should be defined in the Act, but we do think that the ground should only apply if there is a significant likelihood of harassment and if the harassment is serious in nature. The Privacy Commissioner could provide guidance with respect to this new provision, and the list of "specified acts" in the Harassment Act could be of some assistance to agencies in deciding what constitutes harassment.[145]

143 Privacy Act 1993, s 27(1)(d). See *Te Koeti v Otago District Health Board* [2009] NZHRRT 24 for a case in which the Tribunal accepted that there was a risk of harassment serious enough to fall under the "safety" ground for refusal.

144 Privacy Act 1993, s 29(1)(a). See *Patient Requests Names of Nurses who Attended her in Hospital* [2007] NZPrivCmr 7, Case Note 93953; *M v Ministry of Health* Complaints Review Tribunal 12/97, 29 April 1997, 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.

145 Harassment Act 1997, s 4.

RECOMMENDATION

R23 A new provision should be added to section 29, allowing agencies to refuse access where disclosure of the information would create a significant likelihood of serious harassment of an individual.

Mixed information about the requester and others

3.79 Section 29(1)(a) provides that access to personal information may be refused if "the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual". This ground is needed because often information that relates to the individual making the request will also be information about other individuals. Such cases, in which the privacy interests of two or more individuals must be taken into account, were described by the then Privacy Commissioner in *Necessary and Desirable* as "some of the most difficult complaints that come before me". Although he noted that principles for dealing with such cases were developing in Privacy Act and OIA jurisprudence, the Commissioner recommended that consideration be given to providing statutory guidance on the withholding of personal information in cases of "mixed" information.[146] Our provisional view in the issues paper was that statutory guidance on this issue would be difficult to draft and could be too convoluted. We suggested that it might be better for the Privacy Commissioner to provide guidance on this issue.[147]

3.80 There was a consensus in submissions that mixed information does indeed present agencies with particularly difficult challenges, but few agencies saw statutory guidance as the answer, most favouring guidance from OPC instead. Some agencies noted that providing summaries of requested information, leaving out material that involves the unwarranted disclosure of the affairs of others, can be an effective way of dealing with this issue.

3.81 We do not think that the Privacy Act can usefully provide greater guidance with respect to mixed information. As we pointed out in the issues paper, provisions in the Data Protection Act 1998 (UK) that attempt to provide guidance to agencies on this issue are rather long and convoluted,[148] and we doubt that equivalent provisions here would be any simpler. We do, however, think that it would be helpful for the Privacy Commissioner to develop guidance material that would assist agencies in making decisions about requests for mixed information.[149] Since this issue can involve an interface between the Privacy Act (which provides for access by individuals to their own information) and the OIA (which provides for access by individuals to personal information about others held by state sector agencies), the Ombudsmen should be consulted about the development of such guidance.

146 *Necessary and Desirable* at 157–158 (recommendation 52).

147 Issues Paper at 103–104.

148 See particularly Data Protection Act 1998 (UK), ss 7(4), 7(5), 7(6), 8(7).

149 There is already some discussion of this issue on the OPC website: Office of the Privacy Commissioner "Breach of Another's Privacy" < http://privacy.org.nz/breach-of-another-s-privacy > .

3.82 There is, however, one type of case involving mixed information that we think should be specifically provided for in the Act: cases where the request includes information about victims of crime. Often the requester in such cases will be the offender. We have heard from the Police that they are concerned about offenders using the access provisions of the Privacy Act to obtain information about victims, particularly in sexual offence cases. The Police are concerned that providing such information can revictimise crime victims, and that such material is currency in the prison environment. A submission from a government department also referred to a case in which an alleged offender requested information that included information about girls who were his alleged victims, and then placed that information on a website, causing distress to the girls and their families.

3.83 We note that access rights under the Privacy Act are restricted as a consequence of the Criminal Disclosure Act 2008 and the Victims' Rights Act 2002. Section 29(1)(ia) of the Privacy Act allows agencies to refuse access to information that could be sought by a defendant under the Criminal Disclosure Act, or that has been disclosed to or withheld from a defendant under that Act.[150] The Victims' Rights Act provides that Privacy Act access rights do not apply to victim impact statements,[151] and for access to such statements to be restricted.[152] Nonetheless, the overrides of the Privacy Act by the Criminal Disclosure Act and the Victims' Rights Act will not cover all information about victims. In particular, as we note in chapter 9, the Criminal Disclosure Act does not apply to requests for information in relation to proceedings that predate the Act, nor does it apply in respect of allegations of criminal conduct where proceedings have not been commenced. In such situations, information about victims may be obtainable under the Privacy Act, and this could cause distress to those victims. Access to such information could be refused, in whole or in part, under section 29(1)(a), and no doubt this ground is used by agencies in such cases. However, given the uncertainty that exists about refusing access in cases of mixed information, and the particular sensitivity of the information in question, we think a specific ground for refusal should be added to section 29.

3.84 We recommend that a new ground for refusal should allow agencies to withhold personal information requested under principle 6 where that information concerns a victim of an offence or alleged offence, and the disclosure would be likely to cause significant distress, loss of dignity or injury to feelings of the victim, or of a deceased victim's family. The new ground for refusal is likely to be most relevant to victims of sexual offences or violent offences, but it could apply to any victim so long as disclosure of the victim's information would be likely to cause significant distress, loss of dignity or injury to feelings. We think that this new ground for refusal would provide greater certainty to agencies, and would give appropriate recognition to the rights of victims.

150 We discuss the interface between the Privacy Act and the Criminal Disclosure Act further in chs 8 and 9.

151 Victims' Rights Act 2002, s 23(4).

152 Victims' Rights Act 2002, ss 23–27.

3.85 The fact that an access request includes information relating to victims would not necessarily prevent the requester from having appropriate access to that information in some cases. In particular, the Act provides that, where a reason for refusing access applies, the agency may make information that is contained in a document available in a number of ways, including allowing the individual to inspect or view the relevant document, or providing a written or oral summary of the document's contents.[153] Such alternative means of making information available can help to deal with concerns about the further distribution of information about victims.

RECOMMENDATION

R24 The Office of the Privacy Commissioner, in consultation with the Ombudsmen, should develop guidance material in relation to access requests involving mixed information about the requester and other individuals.

RECOMMENDATION

R25 A new provision should be added to section 29, allowing agencies to refuse access where disclosure of the information requested:

- would involve disclosure of information about another individual or a deceased individual who is a victim of an offence or an alleged offence; and
- the disclosure would be likely to cause significant distress, loss of dignity or injury to the feelings of that victim or of a deceased victim's family if they were to learn of it.

Physical or mental health

3.86 Under section 29(1)(c), an agency can refuse access to information requested by an individual if, after consultation undertaken (where practicable) with the individual's medical practitioner, the agency is satisfied that the disclosure of information relating to the individual's physical or mental health would be likely to prejudice that individual's health. Section 29(4) defines "medical practitioner", for the purposes of subsection (1)(c), as a health practitioner registered with the Medical Council of New Zealand as a practitioner of the profession of medicine. Medical practitioners include psychiatrists, but not other mental health professionals. We asked in the issues paper whether section 29(1)(c) should be amended to refer to consulting the individual's psychologist when appropriate, and whether it should refer to consulting with any other health practitioners.

3.87 A preliminary question is whether, if our recommendation above for an expansion of the "safety" ground for refusal to include health is accepted, section 29(1)(c) is still needed at all. Section 29(1)(c) is specifically focused on the disclosure of health-related information to a requester and on the effect of such disclosure on the physical or mental health of the requester, as opposed to the effect on other

153 Privacy Act 1993, s 42. In general, an agency is to make information available in the way preferred by the requester, but it may make the information available in another form if providing it in the form preferred by the requester would prejudice one of the interests protected by the grounds for refusal in ss 27 to 29: Privacy Act 1993, s 42(2)(c).

individuals. It also requires that the agency be satisfied that the information would "prejudice" the individual's health, whereas our proposed amendment of section 27(1)(d) would require likelihood of a "serious threat" to health. We think that "prejudice" is a somewhat lower threshold than "serious threat", but it is balanced by the requirement to consult the individual's medical practitioner, if practicable, so that the decision is informed by expert advice. We consider that the specific ground for refusal in section 29(1)(c) is sufficiently distinct from our recommended amendment to section 27(1)(d) that it should be retained even if our recommendation with respect to the latter section is accepted.

3.88 We received some helpful submissions on the question of expanding the range of practitioners with whom an agency can consult in relation to this ground for refusal. Several submitters supported including psychologists, while several others suggested other ways in which the range of practitioners that can be consulted could be expanded. Based on these submissions, we have concluded that sections 29(1)(c) and 29(4) should be amended to provide for consultation with health practitioners who are able to assess a person's mental state. Section 29(1)(c) is primarily concerned with the effects of information disclosure on an individual's mental state, including the risk that an individual may engage in self-harm. We recommend that section 29(1)(c) be amended to add the words "or relevant health practitioner" after "medical practitioner". We further recommend that section 29(4) be amended to give "health practitioner" the same meaning as in section 5(1) of the Health Practitioners Competence Assurance Act 2003 (HPCAA), and to define "relevant health practitioner" as "a health practitioner whose scope of practice includes the assessment of an individual's mental state". "Scope of practice" is a defined term under the HPCAA. The effect of these amendments would be to provide for consultation, where appropriate, with health practitioners other than medical practitioners, but to limit such consultation to those professions that are covered by the HPCAA and that deal with mental health (including registered psychologists and psychotherapists).

3.89 One submitter raised the question of whether section 29(1)(c) allows for consultation with a medical practitioner other than the individual's own practitioner, and particularly whether an agency can consult a practitioner that it employs. The Complaints Review Tribunal commented in a 1997 decision that:[154]

> If the provision is read as a whole it appears that the purpose of this requirement of consultation is to ensure that the agency seeking to withhold information does so on the basis of sufficient expert knowledge of a requester's medical condition.

The gist of the Tribunal's decision in this case was that section 29(1)(c) imposes a duty on an agency to consult an individual's practitioner (where practicable) if it wishes to rely on this ground for refusal, but that it does not prevent the agency from relying on the evidence of another practitioner who is familiar with the individual if it has good reasons for doing so. We think this is a reasonable interpretation of the provision, and do not think any further clarification is needed with respect to who the agency may consult.[155]

154 *M v Ministry of Health*, above n 144, at 9.

155 See also Office of the Privacy Commissioner "Risk to Mental Health" < http://privacy.org.nz/risk-to-mental-health > .

RECOMMENDATION

R26 Section 29(1)(c) should be amended to add "or relevant health practitioner" after "medical practitioner". Section 29(4) should be amended to define "health practitioner" as having the same meaning as in section 5(1) of the Health Practitioners Competence Assurance Act 2003, and "relevant health practitioner" as "a health practitioner whose scope of practice includes the assessment of an individual's mental state".

Repeated requests

3.90 Sometimes individuals use their principle 6 access rights to repeatedly request the same information. In some cases the request is for information that they have previously been refused access to; in others, the request is for information that has previously been provided to them. Such repeat requests are not always unreasonable: the individual may genuinely wish to obtain information he or she has been refused access to, or may wish to obtain information that has been added to the file since the last request. However, it seems clear that there is a category of repeat request that is vexatious in nature, and is intended to harass the agency concerned or to tie up its resources. In the issues paper we proposed that a new ground for refusal should 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.[156]

3.91 There was strong support for our proposal from submitters, and agencies said that it would help to address a problem that can be a major drain on agencies' time and resources. The only opposition to the proposal came from the Ombudsmen, who questioned whether such a ground for refusal is justified and noted that agencies can already refuse requests that are frivolous or vexatious. The Ombudsmen were concerned that agencies might be too quick to resort to the ground for refusal without first considering whether the information requested is in some way different from that previously supplied, or whether circumstances have changed so as to make it reasonable to give fresh consideration to the request.

3.92 Submissions gave strong support to the view that unreasonable repeat requests are a problem that needs to be addressed, and we do not think that the existing ground for refusing requests that are frivolous or vexatious is adequate for dealing with this problem.[157] A repeat request may not be vexatious on its face, and agencies are likely to feel on firmer ground if there are specific provisions in the Act dealing with this issue. With regard to the possibility that agencies might overuse the new ground for refusal, we note that agencies would not be able to refuse requests if the individual had reasonable grounds for requesting the information again. We therefore recommend that a new ground for refusal should be added to section 29, as proposed in the issues paper.

156 Issues Paper at 105–106.

157 Privacy Act 1993, s 29(1)(j).

This recommendation is in line with an earlier Law Commission recommendation for dealing with a similar problem in relation to the OIA, and we are also proposing such a change as part of our current Official Information review.[158]

RECOMMENDATION

R27 A new provision should be added to section 29, allowing agencies to refuse access if the same information, or substantially the same information, has previously been provided to the requester, or has previously been denied to the requester in accordance with one of the grounds for refusal, provided that no reasonable grounds exist for the individual to request the information again.

Other grounds for refusal

3.93 We asked in the issues paper whether any amendments were needed to the "commercial prejudice" ground for refusal in section 28(1)(b), but based on submissions received we have no recommendations for change to this provision. We have also asked about commercial withholding grounds in our Official Information issues paper,[159] and it is possible that any amendments that come out of that review may have implications for the commercial grounds for refusal in the Privacy Act.

3.94 Some submissions on our issues paper proposed that the confidentiality and privilege grounds for refusal should be broadened. At present, the ground relating to material supplied in confidence relates only to "evaluative material", while legal professional privilege is the only kind of privilege included in the grounds for refusal.[160] Two agencies submitted that the confidentiality ground should be amended to correspond to that in the OIA,[161] which has a broader withholding ground covering information subject to an obligation of confidence. One submitter proposed that the legal professional privilege ground should be broadened to cover other relationships with clients that involve the confidential provision of advice, and suggested that the Privacy Commissioner could be empowered to determine in the public interest that certain organisations are recognised as having privilege in relation to communications with their clients. We do not support these proposals. We think they have the potential to create a large gap in the access regime and to unduly restrict individuals' rights to access their own information, and we are not aware of any specific problems caused by the current scope of the confidentiality and privilege grounds.

3.95 One submission asked for clarification of an element of section 29(1)(b), which allows agencies to refuse access to "evaluative material" supplied in confidence. "Evaluative material" is defined in section 29(3), and covers such things as employment references. The submitter said that there is some uncertainty about

158 Law Commission *Review of the Official Information Act 1982* (NZLC R40, 1997) at 45; Law Commission *The Public's Right to Know: A Review of the Official Information Act 1982 and Parts 1 to 6 of the Local Government Official Information and Meetings Act 1987* (NZLC IP18, 2010) at 109 [*Public's Right to Know*].

159 Law Commission *Public's Right to Know*, above n 158, at ch 5.

160 Privacy Act 1993, ss 29(b) and (f).

161 Official Information Act 1982, s 9(2)(ba).

the meaning of "supplied" in this context. Some agencies have relied on this ground to refuse access to internal file notes or memoranda, but the submitter considered that the provision should be amended to clarify that it only applies to evaluative material supplied by an entity that is separate from the agency itself. Having considered the thorough discussion of this issue by Professor Paul Roth,[162] we do not support the proposed amendment. The Ombudsmen, the Privacy Commissioner and the Tribunal have all taken the view that material can be "supplied" for the purposes of section 29(1)(b) by someone within the agency. The issue turns not on whether the person who supplied the information is inside or outside the agency, but on whether the material was supplied as part of the routine performance of a person's duty or was instead supplied in reliance on a promise of confidentiality. We agree with this interpretation, and think no change is needed.

Part 5 of the Act – procedural provisions for access and correction

3.96 Part 5 of the Act sets out certain procedural matters relating to requests for access to or correction of personal information. We have recommended an amendment to section 45, which is within Part 5, in our discussed of coerced access above.

Charging for correction

3.97 Currently, agencies that are not public sector agencies are allowed to charge for making corrections, in response to requests from individuals, to personal information that they hold.[163] In the issues paper we supported a recommendation of the Privacy Commissioner that the Act should no longer allow such agencies to charge for correction.[164]

3.98 A majority of submissions on this point supported the proposed amendment. It was argued that it is in everyone's interests to ensure that information is accurate, and that charging can serve as a disincentive to requesting corrections, which in turn may lower the integrity and reliability of personal information held by agencies. However, a number of submitters opposed the proposal. They said that, although the right to charge is seldom exercised, it should be retained because of the time and cost involved in some correction requests. It was also suggested that the correction provisions may be abused, and that agencies should be able to charge if the individual making the correction request was the one who originally supplied the incorrect information.

3.99 We remain of the view that agencies should not be allowed to charge for correction, since it is in their own interests to ensure that the information they hold is correct. Principle 7 allows agencies quite considerable leeway in responding to correction requests. There is no obligation on them to correct information when requested to do so;[165] they are only required to take such steps, if any, as are reasonable to ensure that the information is accurate, up to date,

162 Roth *Privacy Law*, above n 99, at [PVA29.12].

163 Privacy Act 1993, s 35(3)(b)(i).

164 The Privacy Commissioner's recommendation is in *Necessary and Desirable* at 184–185 (recommendation 65).

165 See *Plumtree v Attorney-General*, above n 134, at [54], and discussion in Roth *Privacy Law*, above n 99, at [PVA6.10(d)(iii)].

complete and not misleading. They are not obliged to go beyond what is reasonable, having regard to the purposes for which the information may lawfully be used; nor are they required to make any correction if they consider that the information is already correct.

3.100 Where an agency does not make a correction and an individual requests the attachment of a statement of the correction sought but not made, non-public-sector agencies would still be allowed to charge in respect of the attachment of the statement.[166] The argument that it is in the agency's interest to hold correct information, and that it should therefore not be allowed to charge for correction, does not apply to statements of corrections sought but not made. Such statements are for the benefit of the individual concerned rather than the agency, and therefore the agency should be permitted to impose a reasonable charge for attaching a statement.

RECOMMENDATION

R28 Section 35(3)(b)(i), which provides that an agency that is not a public sector agency may charge for correction of personal information, should be deleted.

Extension of time for responding to requests

3.101 The Privacy Commissioner has recommended that the complexity of the issues raised by a request should be added to the grounds on which an agency can extend the time taken to respond to the request beyond the usual limit set by the Act.[167] In the issues paper we supported this proposal, which is based on an earlier Law Commission recommendation with regard to the OIA.[168]

3.102 There was overwhelming support for this proposal from submitters. In supporting the proposal, some submitters referred to matters such as the bulk of information involved or the need to consult. Others mentioned matters that are more properly issues of complexity, such as deciding how to handle mixed information or determining whether information is covered by suppression orders. The only opposition to the proposal came from the Ombudsmen, who did not think that the amendment was warranted. They said that complexity is a subjective concept, and that the proposed ground for extension of time may be used without proper justification if a request simply seems too difficult. In the Ombudsmen's view, "complexity of issues raised" will most often be a reflection either of the volume of information or of the need to consult. They also noted that the OIA currently refers to complexity of issues raised only in relation to extensions of time for responding to requirements imposed by the Ombudsmen,[169] not in relation to extensions of time for responding to requests.

166 Privacy Act 1993, s 35(3)(b)(ii).

167 *Necessary and Desirable* at 195–196 (recommendation 71). Privacy Act 1993, s 41, deals with extension of time limits for responding to requests.

168 Law Commission *Review of the Official Information Act 1982* (NZLC R40, 1997) at 67–68; see also Law Commission *Public's Right to Know*, above n 158, at 117.

169 Official Information Act 1982, s 29A(2)(c).

3.103 We recommend that "complexity of the issues raised" should be added to the grounds for seeking an extension of time limits in section 41(1). Complexity does not refer to the volume of information involved or to the need to consult in order to make a decision, both of which are already covered in section 41(1). An example of a request that could raise complex issues is one in which an agency must decide how to deal with mixed information about the requester and other individuals. While complexity is not currently a ground for extending the time for responding to a request under the OIA, the Law Commission has recommended that it should be. It is also important to note that not only can individuals complain about an agency's decision to extend the time taken to respond to a request,[170] but the agency is required by the Act to inform the requester of his or her right to complain about the extension.[171]

RECOMMENDATION

R29 Complexity of the issues raised by a personal information request should be added to the grounds in section 41(1) on which an agency may extend the time limit for responding to a request.

USE AND DISCLOSURE PRINCIPLES

3.104 Principles 10 and 11 essentially provide that agencies shall not use or disclose personal information for purposes other than those for which it was obtained. They are subject to a number of exceptions which are largely the same for both principles, although there are two exceptions to principle 11 that are not part of principle 10.

Disclosure within agencies

3.105 There is some uncertainty about how principle 11 applies when personal information is disclosed within an agency, such as disclosure between co-workers. A Complaints Review Tribunal decision held that principle 11 does not apply to disclosures within agencies,[172] but this interpretation has been disputed by both the Privacy Commissioner and Professor Paul Roth, who have argued that, if principle 11 is not intended to cover disclosures within agencies, this should be expressly stated in the Act.[173] We asked in the issues paper whether the Act should expressly provide that disclosures within agencies can be covered by principle 11.

3.106 Only a few submitters agreed with the idea of providing that disclosures within agencies can be covered by principle 11, and most opposed it. Submitters who opposed the suggestion said that it would hamstring their ability to share information between different parts of the agency. Several submitters also pointed out that disclosure of information within agencies will be covered by principles 5 and 10 (security and use), and in some cases by agencies' own codes of conduct.

170 Privacy Act 1993, s 66(2)(a)(v).

171 Privacy Act 1993, s 41(4)(c).

172 *KEH and PH v Department of Work and Income* Complaints Review Tribunal 40/2000, 19 December 2000.

173 *Church Elders Disclose Pastor's Marriage Difficulties to Congregation* [2002] NZPrivCmr 8, Case Note 18541; Roth *Privacy Law*, above n 99, at [PVA6.14(c)(xi)].

3.107 On the basis of the strong opposition to the suggested amendment, we recommend no change. We agree that principles 5 and 10 provide protection with regard to the disclosure of information within agencies. There is nothing to prevent an agency from treating internal disclosures as being covered by principle 11, if it makes sense to do so in the agency's particular circumstances.

Disclosure of information that is already known

3.108 The Privacy Commissioner and the Tribunal have taken the view that disclosure of information that is already known by the person to whom it is disclosed 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. Professor Paul Roth has suggested that it is artificial to treat such situations as not involving disclosure, and that it would be better to deal with such situations through a new exception.[174] We asked about this suggestion in the issues paper.[175]

3.109 Opinion in submissions was somewhat divided on this issue, although more submitters opposed the suggestion than supported it. Those who favoured the idea of a new exception for the disclosure of information that is already known said that such an exception would create greater certainty than relying on the interpretation that such cases do not involve disclosure. It was suggested that such an exception might also help to deal with the implied waiver issue, discussed below. Arguments against the suggested new exception were that it:

- is unnecessary;
- would create difficulties in practice, as it may not be easy for agencies to determine the extent to which the individual or agency to whom the disclosure is made does in fact know the information; and
- could have unintended adverse consequences, such as allowing information matching outside the controls of Part 10 of the Act, or allowing legitimate confirmation of information obtained by illegitimate means.

3.110 We recommend no change on this issue. There was insufficient support for a new exception, and we think the same difficulties will be encountered regardless of whether the issue is dealt with by a new exception or, as at present, by treating disclosures of information that the other party already knows as not in fact being disclosures. Establishing whether or not the other party already knows the information will often be difficult, and we do not think that any amendment to the Act can make this assessment any easier.

174 Roth *Privacy Law*, above n 99, at [PVA6.14(c)(i)].

175 Issues Paper at 108–109.

Disclosure and implied authorisation

3.111 A couple of submitters raised the issue of what they called "implied waivers". This is somewhat related to the question of disclosure of information that is already known, as well as to the existing exception to principle 11 for disclosure that is "authorised by the individual concerned".[176] The suggestion of these submitters was that the Act should expressly provide that, where an individual has put some of his or her personal information into the public domain, an agency should be allowed to disclose additional, related personal information about that individual.[177] A typical situation in which the concept of "implied waiver" or "implied authorisation" is seen as being relevant is one in which an individual has gone to the media with a complaint about his or her treatment by an agency. The agency then wishes to disclose personal information about that individual that it holds, in order to "set the record straight".

3.112 In a 1995 report to the Minister of Justice on the release by Ministers of personal information in matters of public controversy, the then Privacy Commissioner commented that whether there are grounds to infer authorisation depends on the circumstances of the case:[178]

> One could imagine public criticism by an individual setting out her alleged personal circumstances, coupled with a demand for the Minister to "explain his actions" might be interpreted as implicit authority to respond to each of the points made even where that involves release of limited personal details. On the other hand, an individual who feels badly treated by a Department and who simply says that could not be considered to have given such a broad authorisation.

More recently, the current Privacy Commissioner considered this issue in a case note on a complaint.[179] A woman spoke to a newspaper about a dispute with a local council in which she was involved. In responding to the newspaper's coverage of the dispute, the council disclosed detailed information about its interactions with the woman, which went well beyond what the woman had herself disclosed. The council argued, in part, that the woman had implicitly authorised the disclosure of her information by initially contacting the newspaper. The Privacy Commissioner, however, observed that the council had disclosed different and more extensive information from that given to the newspaper by the woman, and that the disclosure went well beyond what was necessary to confirm or deny the woman's allegations against the council. The Commissioner therefore formed the opinion that the woman could not be said to have impliedly authorised the council's disclosure.

176 Privacy Act 1993, s 6, principle 11(d).

177 If the agency merely wishes to disclose exactly the same information that the individual concerned has already made public, the "publicly available publication" exception (principle 11(b)) would probably allow for this (although see our recommendation in ch 2 for some narrowing of the scope of that exception).

178 Privacy Commissioner *Legal Framework Surrounding Ministerial Release of Personal Details in Matters of Public Controversy* (report to the Minister of Justice, 1995), quoted in Roth *Privacy Law*, above n 99, at [PVA6.14(h)].

179 *District Council Records not a "Publicly Available Publication" under the Privacy Act* [2009] NZPrivCmr 2, Case Note 100091.

3.113 While authorisation to disclose personal information may sometimes be implied rather than expressly stated, we do not think that the type of situation referred to by the submitters constitutes implied authorisation to disclose additional information, or that the Privacy Act should be amended to allow for disclosure in such circumstances. We understand that agencies will sometimes find it frustrating that they cannot release personal information about an individual in the context of a public controversy, knowing that they hold information that could be used to present a different side of the story. However, we think that a provision for "implied waivers" along the lines proposed by the submitters would not be in the spirit of the Act, and would be open to abuse by agencies. We also note that, if a complaint is made, the fact that the complainant originally made some of his or her personal information public may be relevant to determining whether or not that individual has suffered harm, as required by section 66 of the Act.[180]

Disclosure where there is suspicion of criminal activity

3.114 A financial institution submitted that it would be helpful if a new exception were to be added to principle 11, allowing for disclosure of personal information (possibly only as between registered banks) where there is a reasonable suspicion of criminal activity. The submitter said that, as a responsible financial institution, it has obligations to be alert to suspicious activity that may be linked to criminal offences such as fraud. Often, it said, such situations require discussion and liaison not only with the Police, but also with other banking institutions. It was submitted that, on its face, the "maintenance of the law" exception does not allow for this. The submitter currently deals with this issue by including a term in its contracts whereby customers authorise the institution to disclose personal information in such situations. However, this authorisation provision in contracts has not yet been tested by the Privacy Commissioner, Tribunal or courts.

3.115 The issue that has been raised by the submitter arises from the fact that the "maintenance of the law" exception (which we discuss further in chapter 9) covers "the maintenance of the law by any *public sector agency*, including the prevention, detection, investigation, prosecution, and punishment of offences".[181] Where an agency that is not a public sector agency discloses information in connection with suspected criminal activity, and that disclosure is not directly related to the maintenance of the law by a public sector agency, the exception will not apply. For example, it will not apply to disclosures between banks of their suspicions that a particular customer is engaged in fraud, unless such disclosure is somehow connected to public sector law enforcement activity. The exception will, however, apply to disclosures of information concerning criminal offences from a private sector agency to the Police or other public sector agency.

180 In one such case, the Privacy Commissioner formed the opinion that there had been a breach of principle 11, but that the agency had been restrained in its response and was not responsible for the adverse consequences set out in section 66(1)(b) of the Act: *Client Objects to ACC Disclosures in Response to her Media Statements* [1997] NZPrivCmr 3, Case Note 8649.

181 Privacy Act 1993, s 6, principle 11(e)(i) (emphasis added).

3.116 We do not support the proposal that a new exception should be added to principle 11 to deal with this issue. We are concerned that such an exception could have unintended negative consequences, allowing private sector agencies to share unfounded suspicions about individuals, with potentially serious consequences for those individuals. We do not think that such an exception could realistically be confined to the banking sector (except by way of a code of practice applying to that sector), as other private sector agencies would no doubt ask for the exception to apply to them as well. In our view, the proper course of action if a private sector agency suspects that an individual is engaged in criminal activity is to report those suspicions to the Police or other appropriate public sector law enforcement body.

3.117 There are a number of other options that agencies could pursue, either under existing law or under new legislation:

- Agencies can use the authorisation of the individuals concerned through contracts, as the submitter that raised this issue currently does. While the use of such authorisation may not have been tested in complaints, it is likely to meet the need so long as the terms of the contract are clear.
- For one-off disclosures, agencies can obtain the authorisation of the Privacy Commissioner under section 54.
- Where special provision is needed for a particular industry or sector, agencies in that industry can ask the Privacy Commissioner to develop a code of practice. A code could include a disclosure exception specially tailored to the needs of that industry, and balanced by appropriate safeguards.
- Legislation can be introduced to authorise or require disclosures for the purpose of detecting and investigating particular types of criminal activity. For example, financial institutions and certain other agencies have obligations to report suspicious transactions under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. Such obligations will override the privacy principles by virtue of section 7 of the Privacy Act.

Health and safety exceptions

3.118 Both principle 10 and principle 11 include an exception allowing agencies to use or disclose personal information for purposes other than those for which it was obtained, if such use or disclosure is necessary:[182]

> 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.

3.119 We proposed in the issues paper that the word "imminent" should be deleted from these exceptions.[183] The ALRC has recommended the deletion of "imminent" from equivalent exceptions in the Privacy Act 1988 (Cth), and this

182 Privacy Act 1993, s 6, principles 10(d) and 11(f).

183 Issues Paper at 109–110.

recommendation has been reflected in the Australian Government's Exposure Draft of a new set of Australian Privacy Principles.[184] In the issues paper we noted the following arguments in favour of deleting "imminent":

- Sometimes a threat will be serious, but the harm may not eventuate for some time. For example, the disclosure of genetic information to an individual's relatives could relate to a genetic condition that has very serious consequences, but may not show up for many years.
- An assessment of whether or not a threat is "serious" necessarily involves consideration of the likelihood of a particular outcome, as well as the possible consequences of the outcome.
- An agency wishing to rely on the exception would still need to have reasonable grounds for believing that the use or disclosure is *necessary* to prevent or lessen the threat, not merely that it is convenient or desirable.

3.120 Submissions were overwhelmingly in favour of the proposed amendment. Submitters gave various examples of situations in which the deletion of the requirement that the threat be imminent would allow for the sharing of information about serious threats to health or safety. These included examples relating to child neglect, disease, risk of self-harm, and the disclosure of information about New Zealanders travelling overseas who are in situations of serious but not necessarily imminent danger. Some agencies also saw the proposal as helpful in relation to information sharing between government agencies, which we discuss in appendix 1. In addition, coroners have, from time to time, forwarded to the Law Commission coroners' findings in which failure to disclose information because a threat was not seen as being imminent is considered by the coroner to have contributed to a death.

3.121 A few submitters, while supporting the proposal, suggested safeguards such as replacing "imminent" with another term such as "foreseeable"; developing guidelines which would state that the threat must be foreseeable; or requiring agencies to seek the consent of the individual concerned, where practicable. IHC opposed the deletion of "imminent", stating that "imminent" is included in the exception to ensure that it is used only as a last resort. Without the imminence threshold, IHC submitted:

> agencies might regard a person with an intellectual disability as always or frequently being at serious threat to their life or health as an inherent part of their impairment. Or even a risk to others, in ignorance mostly.

3.122 For the reasons given above, we recommend that "imminent" should be deleted from the health and safety exceptions to principles 10 and 11. We consider that the concerns raised by some submitters can be addressed by spelling out in the Act the elements that must be taken into account in assessing whether or not a threat is "serious". These elements are:

- Likelihood – is it highly probable that the threat will eventuate?
- Consequences – is the threat likely to cause a significant level of harm if it eventuates?
- Imminence – is the threat likely to eventuate soon?

184 *For Your Information* at 859–861; Australian Government "Australian Privacy Principles: Exposure Draft" (2010) principle 6(2)(c).

An agency would not need to believe that all three of these elements are present before it could rely on the exception, but it would need to consider each element in making its assessment. We recommend that these criteria for assessing the seriousness of a threat to health or safety should be spelled out in the Act, and should apply not only to the exceptions to principles 10 and 11 but also to the new health and safety exception which we have recommended for principle 2 and the new health and safety ground for refusal of access which we have recommended for section 27. This recommendation means that agencies will still need to consider the imminence of a threat, but will not be precluded from relying on the exception where disclosure is necessary to deal with a threat that is not imminent but is likely and potentially serious in its consequences.

RECOMMENDATION

R30 The words "and imminent" should be deleted from principles 10(d) and 11(f).

RECOMMENDATION

R31 The Act should set out criteria for assessing seriousness for the purposes of the existing health and safety exceptions to principles 10 and 11, as well as for the new health and safety exception to principle 2 and the new health and safety ground for refusing access in section 27 (see R12 and R22 above). These criteria should be the likelihood, consequences and imminence of any threat to health or safety.

UNIQUE IDENTIFIER PRINCIPLE

3.123 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;
- reassign a unique identifier assigned to the individual by another agency;
- assign a unique identifier to an individual without taking reasonable steps to clearly establish his or her identity; or
- 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.

3.124 Unique identifier is defined as follows:[185]

> **unique identifier** means an identifier—
>
> (a) that is assigned to an individual by an agency for the purposes of the operations of the agency; and
>
> (b) 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.

185 Privacy Act 1993, s 2(1).

3.125 The rationale for principle 12 is not easy to summarise,[186] but it is aimed in part at ensuring that one unique identifier, such as an IRD number, does not become a de facto universal identifier. There are concerns both about the reliability of such de facto universal identifiers, and about the privacy and civil liberties implications of a universal identifier that would facilitate the matching of personal information about individuals held by different agencies. Uncontrolled use of unique identifiers can also create security risks, particularly risks of identity crime. In the United States, Social Security Numbers act as national unique identifiers, and obtaining an individual's Social Security Number can make it much easier to obtain other information about that person. In addition to the issues concerning unique identifiers discussed here, we recommend in chapter 12 an amendment to principle 12 to help address identity crime.

Definitional issues

3.126 We asked in the issues paper whether two terms used in principle 12 need to be defined: "assign" and "identifier".[187] There were relatively few submissions on these issues.

"Assign"

3.127 Principle 12 deals with the assigning of unique identifiers by agencies. In *Necessary and Desirable* the then Privacy Commissioner considered whether "assign" should be defined in the Act. He commented that agencies are sometimes 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 is best to rely on the ordinary meaning of the term and allow the meaning to be clarified over time in real cases.[188]

3.128 There was no consensus in submissions as to whether "assign" should be defined or not. One government agency gave as an example of the difficulties involved with the concept of "assigning" the situation in which Agency A records an identifier assigned by Agency B for the sole purpose of contacting Agency B and enabling Agency B to locate the correct record. OPC made a particularly helpful submission on this question. It said that difficulties of interpretation tend to arise only in relation to principle 12(2), and that this is because that sub-principle uses "assign" twice in slightly different senses. OPC suggested that the interpretational difficulties could be significantly reduced by redrafting principle 12(2), and pointed to the equivalent principle in the Privacy Act 1988 (Cth) which states that an entity must not "adopt as its own identifier" an identifier that has been assigned by another entity.[189] We think that OPC's suggestion is a very promising one, and while we do not propose a particular form of words here, we recommend that the interpretational issues concerning "assign" should be addressed by redrafting principle 12(2).

186 See discussion in Roth *Privacy Law*, above n 99, at [PVA6.15(e)]; *Necessary and Desirable* at 88–89.

187 Issues Paper at 111–113.

188 *Necessary and Desirable* at 89–90.

189 Privacy Act 1988 (Cth), sch 3, National Privacy Principle 7.1.

RECOMMENDATION

R32 Principle 12(2) should be redrafted so that the meaning of "assign" is clearer.

"Identifier"

3.129 While "unique identifier" is defined in the Act, "identifier" is not. We noted in the issues paper a definition of "identifier" that was recommended for inclusion in the Privacy Act 1988 (Cth) by the ALRC.[190] The ALRC's definition of "identifier" would:

- expressly include symbols and biometric information; and
- allow the Privacy Commissioner to determine that something is an identifier.

However, the Australian Government did not accept the ALRC's recommendation that biometric information should be included in the definition, nor did it agree that the Privacy Commissioner should be able to determine that something is an identifier.[191]

3.130 There was little support in submissions for defining "identifier". OPC submitted that the absence of a definition does not appear to be causing any difficulties. There was also a clear message from submissions that biometric information should not be treated as a unique identifier. It was noted that biometric information cannot be "assigned" to an individual in the same way that a number, for example, can be. Several submitters said that the question of regulating biometrics should be considered quite separately from that of regulating unique identifiers.

3.131 We do not recommend that "identifier" should be defined in the Act. The question of regulating biometrics is discussed further in chapter 10.

Principle 12(2)

3.132 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.[192] The previous Privacy Commissioner recommended that the prohibition on reassignment of unique identifiers should apply only to unique identifiers originally assigned by public sector agencies, with the regulation of unique identifiers generated in the private sector to be left to codes of practice.[193] We asked in the issues paper whether the Act should be amended in this way.

3.133 There was only limited support for this proposal, and OPC said in its submission that it no longer supported the proposal. A government agency said that, if controls on unique identifiers originally generated by private sector agencies were to be relaxed in this way, other safeguards would need to be put in place. It was noted, for example, that an individual's cellphone number

190 *For Your Information* at 1040.

191 *Enhancing National Privacy Protection* at 74.

192 Unless the two agencies are "associated persons" within the meaning of subpart YB of the Income Tax Act 2007.

193 *Necessary and Desirable* at 90–91 (recommendation 28).

could be used as a unique identifier. A credit reporting company, while not opposing the suggested change, was concerned at the possibility that a proliferation of codes regulating private sector identifiers could lead to uncertainty for the private sector. On the basis of these submissions, we recommend that principle 12(2) should continue to apply to all unique identifiers, regardless of whether they were originally generated or assigned by the public or the private sector.

3.134 The former Privacy Commissioner also recommended that section 66 be amended so that a wilful breach of principle 12(2) would be an interference with privacy even in the absence of identifiable harm. The rationale for this change was that the existing complaints provisions were unlikely to be effective in relation to principle 12(2) because any breaches were likely to be system-wide rather than individual-specific, and because showing harm in such cases is likely to be difficult.[194] We commented in the issues paper that such an amendment would be unnecessary if our proposal to remove the harm threshold for all complaints was adopted. In this report we are no longer recommending the removal of the harm threshold (see chapter 6). However, we are recommending that the Privacy Commissioner should be given a new power to issue compliance notices. This compliance notice power, discussed in chapter 6, would be an effective means of dealing with systemic issues, and therefore we do not think that any special provision needs to be made for enforcing principle 12(2).

3.135 Principle 12(2) includes no exceptions, apart from allowing for the reassignment of a unique identifier by an agency that is an "associated person" (in terms of the Income Tax Act) of the agency that originally assigned the identifier. We asked in the issues paper whether principle 12(2) should include an exception for statistical and research purposes, and whether it should include any other exceptions.[195]

3.136 Submitters who addressed this question generally supported a new statistical and research exception, and it was strongly supported by Statistics New Zealand. We recommend that an exception for statistical and research uses should be added to principle 12(2). There were some suggestions for other exceptions, but we do not feel that there is a sufficiently clear mandate for those proposed exceptions.

RECOMMENDATION

R33 An exception for the use of unique identifiers for statistical and research purposes should be added to principle 12(2).

194 *Necessary and Desirable* at 91–92 (recommendation 29).

195 Issues Paper at 114.

Principle 12(4)

3.137 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 the identifier was assigned, or for a directly related purpose. It is, nonetheless, common practice for agencies to require people to produce documents such as drivers' licences and passports, which contain unique identifiers, as forms of identification. We therefore asked in the issues paper whether there is any uncertainty about the application of principle 12(4) and, if so, how this should be addressed.

3.138 Submissions on this question indicated that there is indeed some uncertainty about the application of principle 12(4). A non-government organisation said that there is confusion when people are asked to produce a driver's licence as a form of identification as to why this is required, whether agencies are allowed to require it and whether other forms of identification are permitted. A government agency said that simple disclosure of a unique identifier should not cause any harm, but that problems arise when agencies retain and reuse unique identifiers for their own purposes. Another government agency said that there can be problems with defining the purposes for which unique identifiers are assigned, and suggested that a new schedule of such purposes could be added to the Act, with the schedule to be updated by Order in Council. OPC had no proposals for reform of principle 12(4), but said that it focuses on finding practical ways of giving effect to the principle. Such practical solutions include encouraging agencies to accept a range of documents as evidence of identity and to avoid recording any unique identifiers that appear on such documents. OPC said that principle 12(4) continues to be important, and mentioned the serious concerns that have been raised overseas about practices such as nightclubs requiring patrons to have their drivers' licences swiped as a condition of entry, with the data and digital photographs from the licences being copied in the process. Statistics New Zealand asked for an exemption from principle 12(4), noting that the Government Statistician has strong powers to require people to provide information, and that there is no obvious reason why unique identifiers should be excluded from such powers. Statistics New Zealand said that it can operate without such an exemption, but doing so has implications either for the accuracy of its statistics or for the amount of other information that respondents are asked to provide.

3.139 We do not recommend that there be any amendment to principle 12(4), but it does seem that there is some uncertainty and confusion about its application. We note OPC's comment that it is possible to find practical ways of giving effect to the intent of the principle, and that OPC works with agencies to find practical solutions. However, this approach depends on agencies approaching OPC for assistance. We think that, in addition, it would be helpful for OPC to produce guidance material, probably in the form of a user-friendly pamphlet, aimed at agencies that routinely ask customers or clients to provide identification. The pamphlet could set out the kinds of practical solutions OPC mentioned in its submission.

3.140 We do not think there is any need for a schedule of purposes for which unique identifiers have been assigned. It is up to each agency that assigns unique identifiers to document those purposes. With regard to Statistics New Zealand's proposal for an exemption from principle 12(4), we consider that, if such an exemption is justified, it should be provided for in the Statistics Act 1975, not in the Privacy Act.

RECOMMENDATION

R34 The Office of the Privacy Commissioner should develop guidance material on compliance with principle 12(4), aimed at agencies that routinely ask customers or clients to provide identification.

POSSIBLE NEW PRINCIPLES

3.141 While we have recommended various amendments to the existing principles above, overall we think those principles provide an adequate framework for the protection of privacy, and we have not identified any major gaps in them. However, in the issues paper we asked whether any new principles should be added to the Act. We thought that the strongest case existed for adding principles dealing with anonymity and pseudonymity, and with openness, and we discussed those principles at greater length, although we also mentioned some other possible new principles.

Anonymity and pseudonymity

3.142 An individual interacts anonymously with an agency if the individual does not identify himself or herself in any way. If an individual interacts with an agency on the basis of pseudonymity, the individual is not identified by his or her real name but instead uses a pseudonym or alias for the purposes of the interaction. A pseudonym could be specific to the particular interaction. Alternatively, the individual could use the same pseudonym in multiple interactions with the same agency, or in interactions with a range of different agencies. Where a pseudonym is used consistently across multiple interactions, the individual's participation in those interactions can be traced even while his or her identity is kept private. This can be useful, for example, in contexts in which reputation is important, such as online trading.

3.143 Federal data protection legislation in Germany provides for both anonymity and pseudonymity in the following terms:[196]

> Personal data shall be collected, processed and used, and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection.

196 Federal Data Protection Act (Germany), s 3a. English-language version on the site of the Federal Commissioner for Data Protection and Freedom of Information < http://www.bfdi.bund.de/EN/Home/homepage_node.html > . We note that this provision appears to involve the agency anonymising or pseudonymising the information, rather than allowing the individual concerned to interact with the agency anonymously or pseudonymously.

3.144 In Australia, anonymity principles apply nationally in respect of the private sector, and in several states and territories in respect of the public sector.[197] The ALRC has recommended that an anonymity and pseudonymity principle should apply to the public and private sectors, and should be worded as follows: [198]

> Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:
>
> (a) not identifying themselves; or
>
> (b) identifying themselves with a pseudonym.

This recommendation has been accepted by the Australian Government.[199] In New Zealand, the Privacy Commissioner has also recommended the adoption of the ALRC's anonymity and pseudonymity principle.[200]

3.145 The ALRC argued that an anonymity principle encourages agencies to consider, when designing systems, whether they need to collect personal information at all. In addition, there may be public policy benefits from allowing anonymity: for example, it might encourage people to seek medical assistance in some contexts, such as in the case of supplying sterile syringes to injecting drug users. Providing for pseudonymous interactions, the ALRC said, allowed for a more flexible application of the principle, since there will be situations in which it would be impracticable or unlawful for an individual to transact anonymously with an agency but it will be possible to allow the individual to interact under a pseudonym. Furthermore, agencies will be encouraged to build the capacity to interact pseudonymously into their systems.[201]

3.146 We said in the issues paper that anonymity and pseudonymity have important roles to play in the protection of privacy. However, we were undecided about whether the Act needed to make special provision for them, since they could be seen as being already implicit in principle 1. If an agency collects information about a person's identity when it does not need to do so, it is breaching principle 1 by collecting personal information that is not necessary for the agency's purpose. On the other hand, agencies may overlook this particular implication of principle 1 if it is not expressly provided for. We said that, if an anonymity and pseudonymity principle were to be added to the Act, it could be part of principle 1 or could be a separate principle.[202]

3.147 Submissions were fairly evenly divided on the question of recognising anonymity and pseudonymity in the Act. OPC continues to support such a principle, noting that an anonymity principle has applied in the private sector in Australia for some years and that on being reviewed by the ALRC it was found to be suitable

197 Privacy Act 1988 (Cth), sch 3, National Privacy Principle 8; Information Privacy Act 2000 (Vic), sch 1, principle 8; Personal Information Protection Act 2004 (Tas), sch 1, principle 8; Information Act 2003 (NT), sch 2, principle 8; Health Records and Information Privacy Act 2002 (NSW), sch 1, principle 13. The NSW statute is limited to the health sector.

198 *For Your Information* at 708 (UPP 1).

199 *Enhancing National Privacy Protection* at 39; Australian Government "Australian Privacy Principles: Exposure Draft" (2010) principle 2.

200 *1st supplement to Necessary and Desirable* at 23–24 (recommendation 17A, incorrectly numbered 17B); *4th supplement to Necessary and Desirable* at 5–6.

201 *For Your Information* at 692–693, 696.

202 Issues Paper at 116–118.

not only for continuation but also for extension to cover the public sector. A non-government organisation said that such a principle might encourage individuals to share sensitive information, such as in cases involving child safety, and that if individuals are able to use pseudonyms agencies can follow up with them to obtain further information while still allowing individuals not to reveal their identities. A government department supported the principle, but cautioned that agencies will need to take care that they do not promise to deliver a service anonymously or pseudonymously when, in fact, the agency is able to identify individuals. Those submitters who opposed the suggested new principle raised two somewhat contradictory arguments. On the one hand, it was argued that an anonymity and pseudonymity principle was redundant as principle 1 already limits collection of personal information to that which is necessary. On the other hand, submitters argued that such a principle could have negative consequences, including increased compliance costs and risks of fraud, and creating unrealistic hopes of anonymity where this is not in fact practicable. Those opposed to the new principle also said that a strong case for it, in terms of an identified harm or problem, had not been made in the issues paper. Participants in a forum on privacy and the internet organised by Internet NZ did not have a clear view on the possible new principle, but they commented that it is very difficult to be truly anonymous online, and that the Privacy Act currently gets the balance between anonymity and other interests such as law enforcement about right.

3.148 We think an anonymity and pseudonymity principle should be added to the Privacy Act, and that it should be part of principle 1. The new sub-principle would promote control by individuals over their personal information and help to limit unnecessary collection of personal information by agencies. It could also have public policy benefits by encouraging participation in beneficial activities by individuals who would not participate if they had to identify themselves. For example, an individual might provide valuable information, or seek and receive advice about dealing with personal problems, under the protection of anonymity. We think that the new sub-principle would be consistent with principle 1's purpose of limiting the collection of personal information, while at the same time it would flesh out the requirements of that principle. Providing expressly for anonymous or pseudonymous interactions would encourage agencies to consider whether it is possible in particular cases for interactions to take place anonymously or pseudonymously. It would also encourage them to think about whether anonymity or pseudonymity should be provided for when developing policies and processes, and associated materials such as forms.

3.149 We do not think that the new sub-principle would increase compliance costs, partly because it is an elaboration of a principle with which agencies should already be complying and partly because agencies would only need to provide for anonymity or pseudonymity in cases where it is practicable to do so. Likewise, we do not think that the sub-principle would increase risks of fraud or other crime, since individuals would only have the option of interacting anonymously or pseudonymously where this is lawful and practicable. It may be, as one submitter said, that the sub-principle will have little application in some industries, such as banking, where it will seldom if ever be lawful or practicable to allow anonymous or pseudonymous transactions. We do not see it as a problem that the sub-principle is more applicable in some contexts than in others.

3.150 Examples of situations in which it will generally be lawful and practicable to interact with an individual anonymously include the following:

- An individual visits an agency's office or phones an agency to seek general information or to make a general inquiry.
- An individual makes a general complaint to an agency, or fills in a comments form, regarding the level of service provided by the agency. The individual does not wish the agency to follow up with him or her, and is commenting on the level of service generally rather than on the actions of any individual.
- An individual seeks counselling over the phone for a personal problem, but does not wish to establish an ongoing relationship with the agency providing the counselling.

3.151 An example of an interaction that could be conducted pseudonymously is where an agency calls for comments on a particular issue via a moderated online forum. In such a context, there is no reason why individuals should be required to provide their real names, but use of a pseudonym allows both the agency and other commenters to cite the comments of particular individuals by their pseudonyms.

3.152 An Australian commentator has suggested that, in deciding whether it is practicable to deal with an individual anonymously, an agency should consider:[203]

- whether the provision of the product or service requires the individual to be identified;
- whether the provision of the product or service could be improved if the individual's identity was known (for example in relation to a health service where the review of the patient's medical record may assist in treatment);
- whether there will be an increase in cost or time involved in providing the product or service; and
- whether there will be increased risk to the organisation in providing the product or service anonymously (for example, in the event of legal proceedings, the organisation may not be able to provide evidence of correspondence with the individual).

3.153 It may also be helpful to consider whether the effort required to implement an option of anonymity or pseudonymity is proportionate to the value to individuals of providing these options in the particular circumstances. The Act could expressly provide for such a proportionality test, as does the relevant provision in German data protection law, which we have quoted above. The ALRC, for example, considered that where providing an option for individuals to interact anonymously or pseudonymously would require an agency "to make substantial and costly *changes* to its systems, generally this would not be considered 'practicable'". Agencies would, however, be required "to consider the possibility of such an option in the *design* of their systems", in the ALRC's view.[204]

203 J Douglas-Stewart *Annotated Privacy Principles* (3rd ed, Presidian Legal Publications, Adelaide, 2007) at [2–5540], cited in New South Wales Law Reform Commission *Privacy Principles* (R123, Sydney, 2009) at 23.

204 *For Your Information* at 705.

3.154 Some submitters were concerned that the sub-principle would give rise to unrealistic expectations. There are two ways in which this could be the case. First, there will be contexts in which it is not lawful or not practicable to allow for anonymous or pseudonymous transactions. The sub-principle might therefore lead individuals to expect something that some agencies cannot provide. However, none of the principles in the Act provide for absolute rights. Some are qualified by a range of exceptions; others provide that agencies are to take only such steps as are reasonable in the circumstances. There is, therefore, a possibility with any of the principles that an individual will expect something of an agency that, in the particular circumstances, the agency is not in fact required to do or to refrain from doing.

3.155 Secondly, there is a question about whether an individual may believe that he or she is interacting on the basis of anonymity or pseudonymity when in fact the agency is able to use information provided by that individual, perhaps in combination with other information, to identify the individual. We discussed the question of the increasing ease of identification of individuals in our consideration of the definition of "personal information" in chapter 2, and we acknowledge that it is a concern. The new sub-principle should not convey the impression that an agency will necessarily be unable to identify the individual, or that the agency will not under any circumstances attempt to identify the individual. Rather, the principle is concerned with the information that the individual is asked to provide: where lawful and practicable, the agency should allow individuals not to provide any identifying information, or to identify themselves by a pseudonym. In the case of pseudonymous interactions, however, it would make a mockery of the principle if the agency were to allow the individual not to provide his or her real name but at the same time asked for so much other information that his or her identity could easily be discovered.

3.156 With regard to the content of the principle, we think that something similar to the new principle recommended by the ALRC and agreed to by the Australian Government would be appropriate. A new subclause should be added to principle 1 providing that, where it is lawful and practicable in the circumstances, individuals should be able to interact with an agency by either:

(a) not identifying themselves; or
(b) identifying themselves with a pseudonym.

The heading of principle 1 (currently "Purpose of collection of personal information") will probably also need to be amended.[205]

3.157 It is important to note that the sub-principle is concerned with the individual's interaction *with the agency*, and thus is concerned with the information collected by that agency. An agency that, for example, allows an individual to post comments under a pseudonym on its website, but that nonetheless has collected that individual's real name and other identifying details, is not in fact allowing that individual to interact with it pseudonymously.

205 The new heading could, for example, read "Purpose and necessity of collection of personal information".

3.158 If anonymity and pseudonymity are provided for in the Act in accordance with our recommendation, it may be helpful for OPC to issue guidance material on the application of the new sub-principle.

RECOMMENDATION

R35 Principle 1 should be amended by adding a new sub-clause providing that individuals should be able to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do so in the circumstances.

Openness

3.159 Principle 3 already requires agencies to provide certain information to individuals when they collect personal information from those individuals. However, an openness principle would require agencies to make information more widely available (for example, in privacy policies available on their websites) about their handling of personal information. Such a principle was included in the Privacy of Information Bill, which became the Privacy Act, but was dropped. Instead, section 21 of the Act provided for the compilation by the Privacy Commissioner of directories of personal information held by agencies. We recommend in chapter 5 that section 21 should be deleted.

3.160 The ALRC has recommended the inclusion of an openness principle in the Privacy Act 1988 (Cth), and this recommendation has been accepted by the Australian Government.[206] In the issues paper we noted arguments in favour of an openness principle, including that it promotes trust in, and accountability and best practice by, agencies, and that the requirement of notification to individuals at the point of collection may not be adequate for the purpose of assessing an agency's overall practices with respect to information handling. On the other hand, we said that an openness principle could be seen as imposing compliance costs, particularly for small agencies, while for large agencies that collect information for many different purposes, their privacy policies may be so general as to be of little value. We asked for views on whether the Privacy Act should include an openness principle.[207]

3.161 More submitters opposed than supported the addition of an openness principle, although only by a small margin. Arguments in favour of an openness principle centred on the importance of agencies being transparent about their information-handling practices. OPC strongly supported such a principle, arguing that transparency "is an essential feature of a coherent information privacy regime and is an expected component of light-handed regulation that depends upon consumers making informed choices." Youth Law said that an openness principle could help young people to be better aware of the implications of disclosing information and to be better equipped to control the use of their personal information. Submitters who opposed an openness principle were particularly concerned about the compliance costs. A government department said that compliance with the principle would be particularly onerous for small agencies,

206 *For Your Information* at 829 (UPP 4); *Enhancing National Privacy Protection* at 48–50; Australian Government "Australian Privacy Principles: Exposure Draft" (2010) principle 1.

207 Issues Paper at 118–120.

and that it would be preferable to promote transparency through guidance and best practice examples. A submitter from the private sector said that it is not only small agencies that would find compliance a burden. This submitter argued that large agencies collect information for different purposes, and that it is difficult to anticipate and explain these purposes in any meaningful way in a privacy policy. Drafting such a policy is a not insignificant expense.

3.162 We endorse the importance of agencies being as transparent as possible about what they do with personal information. However, we do not support adding an openness principle to the Privacy Act, for two main reasons. First, we do not think it would be reasonable to expect every agency, including very small agencies and individuals (who can be agencies for the purposes of the Act), to develop and publicise a privacy policy. At the same time, setting a threshold at which agencies would be required to comply with an openness principle would be very difficult. The Act could provide that agencies shall take such steps to develop and publicise a privacy policy as are reasonable, having regard to the size and nature of the agency, but we question whether this would provide agencies with sufficient clarity about their obligations. Secondly, we doubt the value of a statutory requirement of openness. We are not questioning the value of privacy policies, and we note that many agencies already have such policies in place. Privacy policies, however, vary widely in quality and usefulness. An openness principle could simply lead some agencies to engage in a box-ticking exercise in compliance, producing privacy policies that are of little use to the individuals whose information they handle. It would be more helpful, in our view, for OPC and appropriate industry bodies to work with agencies to develop user-friendly privacy policies, and to provide templates or examples of good practice. We note that OPC already has some useful guidance material about privacy notices.[208]

Other principles

3.163 In the issues paper we briefly outlined other new principles that could be added to the Act.[209] We did not support these principles, and there was no support for them in submissions. Some of the issues that we discuss later in this report – data breach notification, cross-border data transfers and direct marketing – could also be dealt with by creating new principles. For reasons set out in chapters 7, 11 and 12 we do not favour the creation of separate principles to deal with these issues, although we do recommend the inclusion of a data breach notification obligation in principle 5.

3.164 One of the possible new principles we referred to in the issues paper was a "no disadvantage" principle. Such a principle would provide that agencies should not unfairly disadvantage a person for exercising his or her privacy rights. Former Privacy Commissioner Sir Bruce Slane's submission, while not supporting the addition of a "no disadvantage" principle, suggested that the Act could include an anti-victimisation provision modelled on that in the Human

208 See Office of the Privacy Commissioner "Privacy Notices" < http://privacy.org.nz/privacy-notices > ; Office of the Privacy Commissioner *Questions and Answers about Layered Privacy Notices*. Privacy notices are also discussed in ch 10 of this report.

209 Issues Paper at 120–122.

Rights Act 1993.[210] Such a provision might make it unlawful to treat an individual less favourably than would otherwise be the case because that individual has exercised his or her rights under the Privacy Act, or has declined to do something that would contravene the Act. While we certainly agree that agencies should not disadvantage or victimise individuals for exercising their rights under the Act, we do not think there is a need for a specific anti-victimisation provision in the Act. Such a provision would need to be enforceable in some way, and we note that the provision in the Human Rights Act is enforceable by way of complaint. We suggest that in most cases in which an individual has been disadvantaged as a result of exercising his or her rights under the Privacy Act, the individual will already be in a position to complain about a breach of the Act, and the agency's victimisation of the individual could be taken into account as an aggravating factor in the complaint. Where an individual is victimised by his or her employer for exercising rights under the Act, or for acting in accordance with the Act, remedies will be available in employment law. Such employment law remedies will apply if, for example, a privacy officer is disadvantaged as a result of his or her efforts to bring an agency into compliance with the Act. While victimisation of individuals for exercising rights under the Act could be made an offence, we think that this would be disproportionately severe (especially considering that there is no equivalent offence in the Human Rights Act).

210 Human Rights Act 1993, s 66.

Chapter 4

Exclusions and exemptions

4.1 A range of other rights and interests – such as national security, law enforcement, health and safety, and freedom of information – can justifiably override privacy in particular circumstances. The Privacy Act recognises this fact by providing for exclusions, exemptions and exceptions. Provisions that limit the application of the privacy principles in various ways are consistent with international human rights and privacy instruments, so long as the limitations are authorised and specified by law, are reasonable and are as few as possible.[211] The following distinctions can be drawn between different types of limitations on the application of the privacy principles:

- **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.
- **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.
- **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. 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.

4.2 This chapter is concerned with entities that are excluded from the coverage of the privacy principles by virtue of their exclusion from the definition of "agency", as well as with certain exemptions provided for in Part 6 of the Privacy Act. Some other exclusions, exemptions and exceptions are dealt with elsewhere in this report:

- Some information is excluded from the coverage of the Act by the definitions of "individual" and "personal information", as discussed in chapter 2. In particular, the Act does not generally apply to information about deceased persons or legal persons.

211 Issues Paper at 123–124. See also 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 3 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 5, 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. Such programmes are 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. In appendix 1 we recommend a new framework to cover information matching and other forms of information sharing within government. Under the new framework, government agencies that share personal information with other government agencies as part of an authorised information sharing programme, and in accordance with the terms of the programme, would effectively enjoy an exemption from the operation of the privacy principles.
- As discussed in chapter 8, other laws can override the Privacy Act, in effect creating exceptions to the application of the privacy principles.
- Law enforcement exceptions are discussed in chapter 9.

EXCLUSIONS FROM THE DEFINITION OF "AGENCY"

4.3 "Agency" is defined very broadly in section 2 of the Privacy Act, but the definition also states that it 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.

4.4 The privacy principles refer to information that is collected, held, used or disclosed by an "agency", or to unique identifiers assigned by an agency in the case of principle 12. Therefore, entities that are excluded from the definition of "agency" are not required to comply with the principles and cannot be the subject of complaints of breaches of the principles. There is, however, nothing

to prevent the Privacy Commissioner from commenting or reporting on the actions of such entities, pursuant to the Commissioner's general functions in relation to "the privacy of the individual" under section 13 of the Act (see chapter 5).[212]

4.5 Most of the exclusions from the definition of "agency" seem to us to be unproblematic, and some have their own governing legislation that provides for privacy to be taken into account in decisions about access to information.[213] However, there are some exclusions from the definition of "agency" that we think require further consideration. We asked about these exclusions in the issues paper.

Parliament and Parliamentary agencies

4.6 The House of Representatives and the Parliamentary Service Commission (PSC) are excluded entirely from the coverage of the Privacy Act. Members of Parliament are excluded in their "official capacity". The Parliamentary Service is excluded except in relation to personal information about current or former employees. However, the Office of the Clerk is covered by the Privacy Act.

4.7 In *Necessary and Desirable*, the then Privacy Commissioner noted with regard to the House of Representatives that privacy is protected to some extent by Standing Orders and other rules and practices of the House. He thought that, if any of the privacy principles were to be applied to the House, this should be done by Standing Orders rather than by legislation, and that the initiative for doing so should come from Parliament itself. With regard to MPs, the Commissioner noted that the exclusion of MPs in their "official capacity" went beyond what would apply as an incidence of Parliamentary privilege. For example, MPs' constituency work is part of their activities in their official capacities, and the Commissioner expressed some concern about what happens to personal information held in constituency files when Members lose office. The Privacy Commissioner recommended that an appropriate committee of Parliament should consider the desirability of applying any of the privacy principles to the House or to MPs,[214] and we supported this recommendation in our issues paper.[215]

4.8 The Parliamentary Service provides administrative and support services to the House and to MPs, and administers the payment of funding entitlements for parliamentary purposes.[216] It also provides services to other agencies within the parliamentary complex, including the Office of the Clerk and the Parliamentary

212 For example, in 2007 the Privacy Commissioner reported on the publication of photographs of elderly people and their carers in the New Zealand Nurses Organisation's journal. She noted that the journal fell within the definition of "news medium", and was therefore not subject to the complaints provisions of the Act, but that she was empowered to inquire into the matter by s 13(1)(m) of the Act, which allows the Commissioner to inquire into any matter if it appears that individual privacy may be being infringed: Marie Shroff, Privacy Commissioner *Commissioner Initiated Inquiry under Section 13 of the Privacy Act 1993: Publication of Photographs of Elderly People and their Carers* (2007) at 4.

213 For the courts, see Criminal Proceedings (Access to Court Documents) Rules 2009, r 16(c); District Court Rules 2009, r 3.22(b); Judicature Act 1908, sch 2 (High Court Rules), r 3.16(b). For public inquiries, see Inquiries Bill 2008 (283–2), cl 15(2)(d).

214 *Necessary and Desirable* at 36–39.

215 Issues Paper at 126–127.

216 Parliamentary Service Act 2000, s 7.

Counsel Office. The PSC is made up of MPs, and is chaired by the Speaker. Its functions include advising the Speaker about the nature and objectives of services provided to the House of Representatives and to MPs, and recommending to the Speaker criteria governing funding entitlements for parliamentary purposes.[217] The Privacy Commissioner has recommended that both the Parliamentary Service and the PSC should be subject to privacy principles 1 to 5 and 7 to 12, and that the Parliamentary Service should be subject to principle 6 in respect of current, former and prospective employees and contractors. In the Commissioner's view, the exclusion of the Parliamentary Service and the PSC from the definition of "agency" was intended primarily to place limits on access requests to these two bodies, since such requests could allow indirect access to information prepared for or held by MPs. So long, therefore, as the application of principle 6 was appropriately limited, the Commissioner could see no reason why the privacy principles should not apply to the two bodies.[218] In our issues paper we proposed that the matter be considered by the same committee of Parliament that considers the application of the privacy principles to the House and to MPs.[219]

4.9 We received relatively little comment on the Parliamentary exclusions in submissions, although there was some support for the proposal that the matter be considered by a committee of Parliament. The most extensive submission on these issues was made jointly by the Office of the Clerk and the Parliamentary Service. We have since had further discussions with these two bodies, and these discussions have also informed our recommendations.

4.10 The submission from the Office of the Clerk and the Parliamentary Service observed that the House of Representatives has the exclusive right of control over its proceedings, and that any consideration of applying the privacy principles to the House is a matter for the House itself. There would be an inevitable conflict between privacy protections and the House's privilege of free speech, and resolving such a fundamental conflict is a matter for the House, should it choose to extend privacy protections in the House. The submission noted that, where the House considers it necessary to examine its procedures, the usual practice is for the Standing Orders Committee to inquire and report to the House.

4.11 With regard to MPs, the submission said that it was important to distinguish between the different capacities in which Members act:[220]

- engagement in the proceedings of the House which, as noted above, are subject to parliamentary privilege and to the House's exclusive control of its proceedings;
- other activities in a Member's official capacity, including constituency and caucus activities; and
- personal or purely political activities which, while they may be directly or indirectly associated with a person's position as an MP, are not part of his or

217 Parliamentary Service Act 2000, s 14(1).

218 Bruce Slane, Privacy Commissioner *Report to the Minister of Justice in Relation to the Parliamentary Service Bill* (1999); *1st Supplement to Necessary and Desirable* at 19–20. See also *Necessary and Desirable* at 39–40.

219 Issues Paper at 127–128.

220 These distinctions are discussed in *Necessary and Desirable* at 38, as well as in the submission to the Law Commission from the Office of the Clerk and the Parliamentary Service.

her official functions as a Member. Examples include activities undertaken as a Minister and electioneering activities, as well as activities that are entirely personal (participation in a sporting club, for example). The Privacy Act will already apply to these activities.

4.12 The submission went on to say that any extension of the application of the privacy principles to MPs:

> may have implications on the collection and use of personal information in relation to constituency and political activities, the sharing or transferring of information between parliamentary parties and their political parties, or, members' constituency matters and political activities.
>
> Questions may arise as to the anomalies that may occur for members in not having the privacy principles apply generally to all their activities and difficulties this may create for their staff. This may also have implications for the Parliamentary Service in the management of their staff that work for members and responsibilities those staff may have in relation to members' activities.

If, as the Commission had proposed, a committee of Parliament were to consider extending the application of the privacy principles to MPs in their official activities outside the House, the submission noted that an informal committee could be brought together for this purpose by the Speaker.

4.13 The submission stated that any proposal to extend the privacy principles to cover the PSC would require further discussion with the PSC's members. The application of the privacy principles to the Parliamentary Service would need to be considered at the same time as the issues concerning the PSC and members' official activities outside the House.

4.14 The submission from the New Zealand Law Society drew attention to the handling of personal information by MPs' constituency offices, and commented that it is unclear why this aspect of an MP's official duties should be exempt from the Privacy Act. The Office of the Privacy Commissioner (OPC) continued to support its earlier recommendations on these issues. With regard to the parliamentary service bodies, OPC said that the Law Commission should make a recommendation rather than leaving the matter to be considered by a committee of Parliament. In OPC's view, there is sufficient information now available to allow the Commission to make a recommendation, and change in this area would not raise the same constitutional issues as change directly affecting the House or MPs.

4.15 Before proceeding to discuss our recommendations, we note that the Law Commission has recently, as part of its review of the Civil List Act 1979, recommended that the Official Information Act 1982 (OIA) should be extended to cover information held by the Speaker in his or her role as the Minister responsible for the Parliamentary Service and the Office of the Clerk; the Parliamentary Service; the PSC; and the Office of the Clerk in its departmental holdings. The Commission recommended that the OIA should not apply to the proceedings of the House, information held by the Clerk of the House as agent for the House, information held by MPs in their capacity as MPs, caucus and

caucus committee information, and political party organisational material.[221] The Law Commission is currently reviewing the OIA as a whole, so implementation of these recommendations will await the completion of the OIA review.

4.16 The application of the Privacy Act to Parliament and its associated bodies is in some respects more complicated than the application of the OIA. In the case of the OIA, the question for consideration is the extent to which the OIA's presumption of availability of information is compatible with parliamentary privilege and with the operation of Parliament and its offices. The Privacy Act, on the other hand, imposes controls on the use of personal information. To the extent that the privacy principles limit the collection, use and disclosure of information, they may be at odds with the parliamentary privilege of free speech. At the same time, they may help to protect information that MPs legitimately wish to keep private (such as correspondence with constituents). Matters are further complicated by privacy principle 6 which, like the OIA, provides a right of access to information. There are legitimate concerns about the impact that a right of access to information held by or on behalf of MPs could have on the ability of MPs and political parties to conduct their business. For example, a constituent might complain to an MP about the actions of a third party; if principle 6 applied to MPs, the third party could breach the confidentiality of the constituent-MP relationship by requesting information held about that person by the MP.

4.17 In line with our proposal in the issues paper, we suggest that the application of the privacy principles to the House of Representatives, Members of Parliament in their official capacities, and the Parliamentary Service Commission should be considered by an appropriate committee or committees of Parliament.

4.18 In speaking of "the application of the privacy principles", we do not necessarily mean that the principles would be applied by means of the Privacy Act. Indeed, it would be quite inappropriate to do so in the case of the House, as it would be a breach of parliamentary privilege to make the House subject to supervision by an outside body (the Privacy Commissioner). Any application of the privacy principles to the House would be by way of Standing Orders or some other non-statutory means. We think that the application of the privacy principles to the PSC is also a matter for a committee of Parliament to consider. The PSC is made up of MPs, and the application of the privacy principles to it is best considered together with the wider issues concerning the House and MPs. Ideally, the issues concerning the application of the privacy principles to the House, MPs and the PSC would all be considered by the same committee. However, we note the point made in the submission from the Office of the Clerk and the Parliamentary Service, that matters concerning the procedures of the House are normally considered by the Standing Orders Committee whereas the issues concerning MPs (and, presumably, the PSC) could be considered by an informal committee brought together by the Speaker. We leave it to the House to decide on the most appropriate committee or committees to consider these matters.

221 Law Commission *Review of the Civil List Act 1979: Members of Parliament and Ministers* (NZLC R119, 2010) at 37–42.

4.19 With regard to the Parliamentary Service, we have taken into account the recommendations of the Privacy Commissioner and our further discussions with the Parliamentary Service, and we now think that the Privacy Act should apply more generally to the Service. The main concern about applying the Privacy Act to the Parliamentary Service is that the Service holds a great deal of information on behalf of MPs. We have already noted the concerns about applying the Act to MPs, and recommended that the application of the privacy principles to MPs should be considered by a committee of Parliament. It would be anomalous, therefore, if we were to make a recommendation with regard to the Parliamentary Service that would have the effect of making a significant body of information held on behalf of MPs subject to the Act. We recommend that the Parliamentary Service should be covered by the Act, but only in respect of its departmental holdings (including information about employees and contractors). Information held by the Parliamentary Service as an agent for MPs should continue to be excluded from the coverage of the Act. We suggest that our recommendation could be implemented by removing the Parliamentary Service from the list of entities excluded from the definition of "agency", but providing elsewhere in the Act that information held by the Parliamentary Service on behalf of MPs shall be deemed to be held by the MPs and not by the Parliamentary Service.[222] So long as MPs continue not to be covered by the Privacy Act, this will put such information outside the Act's coverage. We are encouraged to learn from the Parliamentary Service that they already promote compliance with most of the privacy principles (to the extent that it is practicable to do so in the circumstances), including in relation to information held on behalf of MPs.

RECOMMENDATION

R36 The Privacy Act should apply to the Parliamentary Service, but only in respect of its departmental holdings. Information held by the Parliamentary Service on behalf of Members of Parliament should not be covered by the Privacy Act.

Ombudsmen

4.20 The Privacy Commissioner has recommended that the Ombudsmen should be made subject to the Privacy Act,[223] and we supported this recommendation in our issues paper. We simply believe that, as a matter of principle and for the sake of consistency, all organisations should be subject to the Privacy Act unless there is good reason to the contrary. The courts are subject to it (except in their judicial functions); so are the other officers of Parliament, the Auditor-General and the Parliamentary Commissioner for the Environment. So the question is why the Ombudsmen should not be. Most submissions that responded to this proposal supported the change, but the Ombudsmen argued against it for the following reasons:

- The Ombudsmen are the "last line" check on the exercise of executive power, and should not be subject to investigation by an agency such as the Privacy Commissioner that is itself subject to the Ombudsmen's jurisdiction.

222 A provision concerning the holding by Parliamentary Service of information on behalf of MPs could be included in section 3, which deals with the circumstances in which information is considered to be held by an agency.

223 *Necessary and Desirable* at 42–43.

- The Ombudsmen Act already contains sufficient protections with respect to the handling of personal information.[224]
- Providing for principle 6 access rights in respect of personal information at the margins of the Ombudsmen's secrecy requirements could impede the Ombudsmen's ability to carry out their statutory functions of resolving complaints in a thorough and timely manner.

The Ombudsmen were willing to accept the application of privacy principles 6 and 7 to personal information about employees and former employees. However, they said that if such access and correction rights were to be legislated for, it would be preferable for this to be done by incorporating principles 6 and 7 in the Ombudsmen Act, rather than providing for complaints under the Privacy Act.

4.21 As to the first point, we do not think that there is anything unusual or problematic in making one complaints body subject to investigation by another. For example, the Privacy Commissioner is subject to complaints to the Human Rights Commission and the Ombudsmen.[225] The Ombudsmen's activities would not become open to general review by the Privacy Commissioner, but only to investigation of complaints in the specific area of privacy protection. As the former Privacy Commissioner has said, making an institution subject to a complaints mechanism "does not undermine public confidence in it but rather strengthens it."[226]

4.22 On the second of the Ombudsmen's points, we consider that the existing provisions in the Ombudsmen Act do not cover all the ground in the Privacy Act. The Ombudsmen's secrecy provisions do not, for example, deal with matters such as collection and retention of personal information that are covered by the privacy principles.

4.23 With regard to the possible impact of principle 6 access rights on the Ombudsmen's exercise of their statutory functions, we think that sufficient protection for the Ombudsmen's complaints-resolution functions is provided by the combination of the secrecy obligation in the Ombudsmen Act[227] (which would override the Privacy Act by virtue of section 7) and section 55(d) of the Privacy Act, which provides that nothing in principles 6 and 7 applies in respect of:

> information contained in any correspondence or communication that has taken place between the office of the Ombudsmen and any agency and that relates to any investigation conducted by an Ombudsman under the Ombudsmen Act 1975 or the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, other than information that came into existence before the commencement of that investigation.

4.24 We therefore recommend that the Ombudsmen should be made subject to the Act.

---

224 Specifically, the Ombudsmen cited s 21(2) of the Ombudsmen Act 1975, which requires the Ombudsmen and their staff to maintain secrecy. With regard to access requests, they cited certain provisions which allow or require the Ombudsmen to make information available to complainants concerning what has been done in respect of their complaints: Ombudsmen Act 1975, ss 17, 21(4), 24(2).

225 In ch 6 we recommend that there should be no change to the Ombudsmen's power to investigate the Privacy Commissioner's handling of complaints.

226 *Necessary and Desirable* at 43.

227 Ombudsmen Act 1975, s 21.

RECOMMENDATION

R37 The Ombudsmen should be deleted from the list of entities excluded from the definition of "agency".

News media

4.25 "Agency" is defined as not including "in relation to its news activities, any news medium." "News activity" is defined to mean:

(a) the gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public:

(b) the dissemination, to the public or any section of the public, of any article or programme of or concerning –

(i) news:

(ii) observations on news:

(iii) current affairs.

"News medium" is defined 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.

4.26 We said in the issues paper that this exclusion is justified. The free flow of information through the media is vital to the life of a free and democratic society, and is supported by the protection of freedom of expression in the New Zealand Bill of Rights Act 1990.[228] It is difficult to see how the media could perform this role effectively if it were subject to the Privacy Act's principles. Those principles are ill-aligned to the media function. For example they provide that an agency must collect personal information about an individual directly from the individual; it must allow the individual access to the information it holds about him or her; and it must not disclose the personal information it holds to anyone else. "Personal information" is defined simply as "information about an identifiable individual"; and while all the principles are subject to exceptions, those exceptions are limited and specific. Not only could the media not operate effectively in such a context: they could barely operate at all. This, however, is not to say that the media do not need to respect privacy. Of course they do. They are subject to the tort of invasion of privacy if they publish private facts in an objectionable way. They are also governed by their own regulators – the Broadcasting Standards Authority and the Press Council – which apply their own privacy principles specially tailored to the media.[229] It is important that specialist regulators regulate the media. Privacy is only one of the standards those regulators enforce: others are good taste, fairness, and balance, standards

228 New Zealand Bill of Rights Act 1990, s 14: "Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form."

229 See Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC IP14, 2009) at 64–69 [*Invasion of Privacy*].

which sometimes overlap with privacy. It would be quite artificial to pluck privacy alone away from the media regulators and give it to the Privacy Commissioner.[230]

4.27 The Privacy Act is not alone among New Zealand statutes in granting the media or journalists an exemption from its provisions,[231] and similar exemptions are also found in overseas privacy laws.[232]

4.28 No submitters disagreed with our view that the news media exclusion should remain in the Act. OPC agreed that it should remain for the time being, although it said that the matter should continue to be re-examined from time to time. We think there should be no change to the general principle that the news media, in relation to their news activities, should not be subject to the privacy principles. However, there are some further issues about the news media exclusion that we now examine.

"News activity"

4.29 A "news medium" is excluded from the coverage of the privacy principles only in relation to its "news activities". We asked in the issues paper whether "news activity" could be defined more precisely. Although it is a defined term in the Act, there are still several possible interpretations of the scope of "news activity":[233]

- that the media organisation is protected so long as it is 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); or
- 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).

4.30 A genre or public interest test might lead to the conclusion that, for example, a television reality programme or a humorous column in a newspaper would fall outside the news media exclusion. There have been relatively few complaints in which the scope of the news media exclusion has arisen. In those cases where it has been considered, the Privacy Commissioner and the Tribunal have taken a broad view of the scope of "news activity", and have held that the *National Business Review*'s "Rich List" and the consumer affairs programme "Target" are covered by the exclusion.[234] In the issues paper we proposed that the current

230 Note, however, that while the Privacy Commissioner cannot investigate complaints about the media, the Commissioner could still inquire into, and report on, matters involving the media under his or her general powers of inquiry and report: see n 212 above.

231 See for example Fair Trading Act 1986, s 15; Financial Advisors Act 2008, s 12(a); Criminal Justice Act 1985, s 138(3); Criminal Procedure (Reform and Modernisation) Bill 2010 (243–1), cl 202.

232 See for example 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).

233 See Elizabeth Paton-Simpson "The News Activity Exemption in the Privacy Act 1993" (2000) 6 NZBLQ 269.

234 *Talley Family v National Business Review* (1997) 4 HRNZ 72; *TV Technician Complains About Being Covertly Filmed for a TV Programme* [2003] NZ PrivCmr 24, Case Note 38197.

definition should not be changed, leaving it to the Privacy Commissioner and the Tribunal to decide what constitutes "news activity" on a case-by-case basis. We commented that the line between news and entertainment is increasingly unclear, and that it would be very difficult to clearly distinguish news from other media activities.

4.31 Most submitters on this question agreed that the current definition should not be changed. The Media Freedom Committee of the New Zealand section of the Commonwealth Press Union ("the Media Freedom Committee") argued that "news activity" should continue to be viewed broadly, and that it would be very difficult to define it with greater precision. Similarly, the Screen Production and Development Association of New Zealand (SPADA) agreed with our view that it is increasingly difficult to distinguish between news and entertainment as genres continue to evolve, and that it is best to make judgements case-by-case. However, the Press Council thought that there might be a case for amending the current definition to make it clear that the "capacity" test is the correct one. The "public interest" and "genre" tests would, they asserted, be too restrictive on the news media.

4.32 A more fundamental point was raised in a submission by a United Kingdom-based academic specialising in privacy law, Dr David Erdos, who argued that the exclusion should not be limited to the media and "news activities" at all. He considered that the exclusion should cover any form of publication to the public or a section of the public, providing the publication was not against the public interest. His proposed exclusion would thus cover a wide range of journalistic, literary, artistic and research works, including "new" media such as blogs and social networking sites. He noted that the equivalent exclusion in the Data Protection Act 1998 (UK) is broader than New Zealand's, covering "journalistic, literary or artistic material",[235] although Erdos would also include publication of research work. He is thus proposing an exclusion that is much broader than the current "news media" exclusion in the Privacy Act, although it would be limited by a public interest test.

4.33 The issues raised by David Erdos are not without merit. It might seem anomalous that a journalist who writes a story in the newspaper is protected by the news media exclusion, but if the journalist (or someone else) were to tell the same story in a book he or she would not be protected. It can also be argued that freedom of literary and artistic expression, and the freedom of researchers to publish their findings, are just as fundamentally important as media freedom. However, while we do not deny the importance of such forms of expression, we do not recommend an expansion of the current exclusion in the way proposed by Erdos for several reasons. First, media freedom is generally considered to have a particularly important place in the life of a democratic community. The news media (using that term broadly) play a crucial role in informing day-to-day discussion and debate on political, social, cultural and economic issues. Secondly, while the news media are exempt from the Privacy Act, they are subject to other forms of regulation and to complaints bodies. The same is not true of other forms of expression. We recommend below that the news media exclusion should be limited to those media that are subject to a code of ethics and a complaints

235 Data Protection Act 1998 (UK), s 32.

procedure. Thirdly, the amendment proposed by Erdos would involve a major change to the Act, one for which we simply do not have a mandate, since no other submitters proposed such a change. The current exclusion is quite well understood, and we do not wish to upset the existing balance in the Act without clear evidence that there is support for doing so.

4.34 The consensus among submitters was that the definition of "news activity" should remain unchanged, and we recommend accordingly. In most cases we think it will be clear whether or not a medium is engaged in news activity, and cases at the margins are unlikely to be assisted by any attempt at clarifying the boundaries of "news".

"News medium"

4.35 When the Privacy Act was enacted, it was reasonably clear that the news media exclusion applied to "traditional" media: newspapers, magazines, radio and television. Since then, however, there has been a proliferation of "new" media, mainly on the internet, including blogs, news sites, social networking sites, microblogging sites such as Twitter, and video-sharing sites such as YouTube. Should such non-traditional media be able to take advantage of the Privacy Act's news media exclusion?

4.36 On the face of the definitions of "news medium" and "news activity", there is nothing to prevent online publications that are not associated with a print publication or a broadcaster from benefiting from the news media exclusion. Many such publications are involved in the gathering, preparation or compiling, and dissemination of news, current affairs and, especially, "observations on news". They disseminate such material to the public or to a section of the public. They would thus appear to be engaged in "news activity". There could be a question about whether such news activity constitutes their "business", or part of their business, for the purposes of the definition of "news medium", but it is certainly arguable that at least some online publications are engaged in the "business" of news.

4.37 If some online publications are news media for the purposes of the Privacy Act, and are therefore excluded from the coverage of the privacy principles, there is a problem: there will be no avenue of complaint for individuals who feel that their privacy has been infringed by such publications, apart from the very expensive and uncertain route of suing in tort. By contrast, there are complaints avenues open in respect of the "traditional" media: the Broadcasting Standards Authority and the Press Council. The Press Council accepts complaints concerning the websites of newspapers and magazines, but has so far not dealt with complaints about "web only" publications. There is no other regulatory or self-regulatory body governing online publications.

4.38 In the issues paper we asked what should be done about this situation, and whether the definition of "news medium" should be confined in some way. Should it, for example, be confined to the print and broadcast media? Should it be confined to media that are subject to a code of ethics and a complaints procedure administered by an appropriate body? No submitters supported confining the definition to the print and broadcast media, and we agree that it would be a mistake to do so. Such an approach would be anachronistic in

today's media environment, and would risk creating anomalies: it would make no sense if the Privacy Commissioner could investigate a complaint about the online version of a newspaper article but not the print version of the same article. There was, however, some support for restricting the definition of "news medium" to news media that are subject to a code of ethics and a complaints procedure. The Media Freedom Committee reported that there were mixed views among its members on this issue, but that the consensus view favoured the approach based on codes of ethics and complaints procedures. This approach was also supported by OPC. However, Fairfax Media said that there should not be any attempt to confine the definition of "news medium", and questioned whether there is a problem with the current situation. They noted that many websites have their own codes and procedures for dealing quickly and effectively with complaints about material posted on the sites, and gave as an example the website Trade Me.[236]

4.39 We think that the definition of "news medium" should be limited to media that are subject to a code of ethics that deals expressly with privacy, and to a complaints procedure administered by an appropriate body. By "appropriate body" we mean a body that is separate from the media organisation itself: an agency that polices its own code of ethics would not qualify. The body administering the complaints procedure need not be a statutory one, however: it could be an industry-initiated, self-regulatory body like the Press Council. The obvious examples of complaints bodies at present are the Broadcasting Standards Authority and the Press Council, but other such bodies may arise in future specifically for the online media.

4.40 This recommendation would, we believe, deal with the potential gap in privacy protection which we have identified above: the fact that at present some publications could fall within the news media exclusion while not being subject to any other accessible complaints jurisdiction. Our recommended approach is similar to that taken in the Federal Privacy Act in Australia.[237] It is also consistent with the Law Commission's recommendation, in its report on suppressing names and evidence, with regard to defining those members of the media who are entitled to remain in court when an order is made excluding the general public.[238]

4.41 Participants in a discussion of privacy and the internet, organised for us by Internet NZ, told us that the challenges posed by the definition of "news medium" are part of the wider issue of reviewing the regulation of the news media in the internet age. We agree, and in October 2010 the Law Commission received a reference to undertake a review of the adequacy of the current regulatory regime for the news media to deal with new and emerging forms of media. However, we can see no reason why our recommendation with respect to the definition of "news medium" in the Privacy Act should not proceed ahead of the completion of our "new media" project.

236 Trade Me made its own submission, which did not address the questions about the news media exclusion.

237 Privacy Act 1988 (Cth), s 7B(4)(b).

238 Law Commission *Suppressing Names and Evidence* (NZLC R109, 2009) at [5.21]. This recommendation has now been incorporated in the Criminal Procedure (Reform and Modernisation) Bill 2010 (243–1), cl 202, which provides that orders to clear the court may not, in most circumstances, exclude members of the media. Clause 202(2) defines "member of the media" as meaning a media reporter who is subject to a code of ethics and to the complaints procedures of the Broadcasting Standards Authority or the Press Council, or any other person reporting on proceedings with the permission of the court.

Radio New Zealand and Television New Zealand

4.42 Radio New Zealand (RNZ) and Television New Zealand (TVNZ) fall within the definition of "news media" for most purposes, but the definition states that they are not news media for the purposes of principles 6 and 7. This means that RNZ and TVNZ are subject to requests by individuals for access to information about themselves held by these two organisations, and to requests for correction of personal information. This provision was included in the Privacy Act in order to continue rights that had previously existed under the OIA. When the Privacy Act was enacted, access and correction rights of individuals with respect to personal information held by public sector bodies (including RNZ and TVNZ) were removed from the OIA and replaced by the access and correction provisions of the Privacy Act.

4.43 In the issues paper, we proposed that the limiting reference to RNZ and TVNZ in the definition of "news medium" should be removed. We argued that the right of access to and correction of personal information held by the state broadcasters can have a negative effect (a delaying effect, at the very least) on the dissemination of news. It can lead to an application for an injunction,[239] for example, or to a lengthy stalling debate about whether information held is accurate or not.[240]

4.44 There was quite widespread support in submissions for our proposal, including from all of the media submitters. The Media Freedom Committee said that the justification for the news media exclusion in respect of principles 6 and 7 applies just as much to RNZ and TVNZ as it does to other media organisations. They also noted that another state broadcaster, Māori Television, is not subject to the same limitation.[241] A joint submission from RNZ and TVNZ also argued that they had just as much reason to be exempt from principles 6 and 7 as do the private sector news media. They said that:

> The ability of a person to apply to access the fruits of a news investigation about themselves, and to correct anything they may disagree with, can restrict the investigation and dissemination of news and current affairs. If made prior to broadcast, it may delay broadcast while the accuracy of information collected is determined through the complaint/proceedings processes provided under the Act.
>
> In our experience requests for access to personal information in news files has invariably been for a collateral purpose – to attempt to delay broadcast, discourage the continuation of an investigation, or to bolster a complaint to the Broadcasting Standards Authority or proceedings, either already in existence or in contemplation.

239 In this context, it is important to note 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)), and that RNZ and TVNZ are public sector agencies in terms of the Privacy Act (Privacy Act 1993, s 2(1), definitions of "public sector agency" and "organisation"; Official Information Act 1982, sch 1).

240 One complaint to the Privacy Commissioner involving an access request for personal information to TVNZ is discussed in John Burrows and Ursula Cheer *Media Law in New Zealand* (6th ed, LexisNexis, Wellington, 2010) at 380.

241 The Māori Television Service is a statutory corporation established by the Māori Television Service (Te Aratuku Whakaata Irirangi Māori) Act 2003. While its origins are different from those of RNZ and TVNZ, Māori Television is established and funded by the Crown, just as RNZ and TVNZ are. It is subject to the OIA: Official Information Act 1982, sch 1.

The submission concluded that the application of principles 6 and 7 to RNZ and TVNZ was an unjustified restriction on freedom of the media, and that there is no principled basis for denying the two state broadcasters the protection offered to their private sector counterparts, and to Māori Television.

4.45 However, our proposal was opposed by OPC. OPC said that the proposal would remove access and correction rights with respect to personal information held by the state broadcasters that New Zealanders had enjoyed for two decades. Parliament has, OPC said, repeatedly made clear that state-owned enterprises have additional obligations of transparency that do not always apply to their private-sector competitors. OPC questioned the contention that access and correction rights had made RNZ and TVNZ subject to injunctions and delaying tactics. It also pointed out that RNZ and TVNZ are subject to the OIA, unlike other media companies, and that removing access and correction rights under the Privacy Act would therefore create an anomaly: individuals could not request information about themselves from the state broadcasters, but third parties could request information about those same individuals under the OIA. Moreover, companies would continue to have access and correction rights, under the OIA,[242] to information about themselves held by RNZ and TVNZ, while natural persons would not.

4.46 We remain of the opinion that RNZ and TVNZ should not be subject to the access and correction principles under the Privacy Act. However, we are troubled by the issues concerning the interface with the OIA raised by OPC. Our preferred solution is not to modify our proposal with regard to the Privacy Act, but to consider, in our review of the OIA, whether corresponding changes should be made to that Act. We shall need to consider whether the OIA should be amended to provide that TVNZ, RNZ and Māori Television are not covered by the OIA in respect of information held in connection with their "news activities", which would be defined in the same terms as in the Privacy Act. There are similar carve-outs for state broadcasters in freedom of information legislation overseas.[243]

4.47 As a consequence of our recommendation to delete the limiting reference to RNZ and TVNZ from the definition of "news medium", we also recommend the deletion of section 29(1)(g) of the Privacy Act, which allows RNZ and TVNZ to withhold information requested as part of an access request if disclosure would be likely to reveal a journalist's source.

242 Official Information Act 1982, ss 24, 26.

243 Freedom of Information Act 2000 (UK), sch 1, Part 6: the Act applies to the British Broadcasting Corporation and other state broadcasters "in respect of information held for purposes other than those of journalism, art or literature"; Access to Information Act RSC 1985 c A-1, s 68.1: the Act does not apply to information under the control of the Canadian Broadcasting Corporation "that relates to its journalistic, creative or programming activities, other than information that relates to its general administration"; Freedom of Information Act 1982 (Cth), sch 2, Part 2: the Australian Broadcasting Corporation and the Special Broadcasting Service Corporation are exempt in relation to their program material and datacasting content.

RECOMMENDATION

R38 The definition of "news medium" should be amended so that the news media exclusion from the Privacy Act applies only to media that are subject to a code of ethics that deals expressly with privacy, and to a complaints procedure administered by an appropriate body.

RECOMMENDATION

R39 The limiting reference to Radio New Zealand and Television New Zealand should be removed from the definition of "news medium", and consequentially section 29(1)(g) should also be deleted.

EXEMPTIONS IN PART 6 OF THE ACT

4.48 Part 6 of the Privacy Act provides for certain specific types of exemption, which we discuss here. It also deals with codes of practice, which are discussed in chapter 5.

Section 54 – exemptions authorised by the Privacy Commissioner

4.49 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 must 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.

4.50 The Commissioner reports annually on section 54 applications.[244] There are only a few applications each year, and it seems that many applications are not granted. A common reason for declining applications is that the Commissioner considers that the exemption applied for is unnecessary, since the agency's objectives can already be achieved without breaching the privacy principles.

4.51 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. The Commissioner has issued a Guidance Note for applicants seeking section 54 exemptions, and this Note states:[245]

> 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

244 See for example Office of the Privacy Commissioner *Annual Report 2010* (Wellington, 2010) at 42–43.

245 Office of the Privacy Commissioner "Guidance Note to Applicants Seeking Exemption Under Section 54 of the Privacy Act 1993" (1997) at [3.4].

an agency's activities, it is likely that an exemption will be inappropriate. Consideration should instead be given to seeking a code of practice.

4.52 We asked in the issues paper whether section 54 should be amended to allow for ongoing exemptions. We proposed that it should not be amended in this way, for the following reasons:

- There is no evidence of a problem: the privacy principles already have a considerable amount of flexibility, and where the principles need to be modified for a particular sector there is the option of developing a code of practice. The experience with the existing section 54 provision suggests that many applications would be turned down by the Privacy Commissioner on the grounds that what the agency seeks to do is already allowed under the Act.
- A power to authorise ongoing exemptions would give the Privacy Commissioner significant powers to modify the terms of the Act. While this is already true of the power to issue codes of practice, these include procedural safeguards such as consultation and notification provisions. In addition, we are recommending in this report that codes of practice should be approved by Cabinet. If similar safeguards were put in place for section 54 exemptions, it is hard to see how such exemptions would differ from codes.
- While it would be possible to justify ongoing exemptions on public interest grounds,[246] it would be more difficult to assess ongoing exemptions that purport to involve "a clear benefit to the individual concerned".[247] It would also be difficult to apply the provision stating that an exemption shall not be authorised by the Commissioner where the individual concerned has refused to authorise the collection, use or disclosure.[248] This provision seems to contemplate a one-off opportunity to refuse consent, and would be problematic in the context of an ongoing exemption.

4.53 Only one submitter, a credit reporting firm, disagreed with our proposal that section 54 should continue to be limited to one-off exemptions. This submitter firstly disagreed with the Privacy Commissioner's interpretation of section 54, arguing that the reference to "the special circumstances of the case" should not preclude the granting of ongoing exemptions. Secondly, they disagreed with the contention that there is no need for a power for the Privacy Commissioner to grant ongoing exemptions. They said that, from time to time, they wish to disclose information to a specific client but are unable to do so in compliance with the Act. An amendment to the Credit Reporting Privacy Code would be possible, but this is an involved process and seems excessive given that the exemption would apply to a single client while the Code applies generally to the field of credit reporting. The submitter was not convinced that limited use of ongoing exemptions would require any special safeguards, although limitations could certainly be placed on the exemption to ensure that it applies only in special circumstances.

246 Privacy Act 1993, s 54(1)(a).

247 Privacy Act 1993, s 54(1)(b).

248 Privacy Act 1993, s 54(3).

4.54 Despite the points raised by this submitter, we continue to believe that section 54 should only allow for one-off exemptions to deal with specific circumstances. There is nothing to stop an agency from making repeated requests for exemptions under section 54, but each request should be considered separately by the Privacy Commissioner. If a need for an exemption arises repeatedly, however, a code is the most appropriate way of providing for it, no matter how specific the exemption may be. To give the Privacy Commissioner a power to grant ongoing exemptions would be constitutionally questionable, since it would mean that an appointed official could effectively change the law passed by Parliament. The same objection can be made with respect to codes of practice under the Act, but there are a range of procedural safeguards in relation to codes, and in addition we recommend in chapter 5 that codes should be approved by Cabinet. We note that we also raised the option of expanding the Commissioner's section 54 power in the chapter of the issues paper dealing with information sharing,[249] as a possible way of dealing with the matters discussed in appendix 1 of this report. There was little support for this option among submitters, and we are satisfied that most users of the Act see no need for section 54 to go beyond one-off exemptions.

4.55 We also asked in the issues paper whether section 54 should be amended to allow the Commissioner to grant exemptions from privacy principles other than 2, 10 and 11. We proposed that exemptions from principle 9 should also be allowed, and this proposal was supported by submitters. The Privacy Officers' Round Table said that section 54 should provide that the Commissioner may grant exemptions from any of the principles. A government department proposed that exemptions from principle 12 should be able to be granted. We think a power to grant exemptions from any of the principles would go too far, and that any exemption-granting power should be limited as much as possible. Principle 1, for example, is fundamental to the whole operation of the Act, and we do not think the Commissioner should be able to grant exemptions from this principle. We do, however, think that the Commissioner should be able to grant exemptions from principles 9 and 12. The Privacy Commissioner's *Necessary and Desirable* review asked whether the section 54 power should apply to these two principles, although in the end the Commissioner recommended that it be extended only to principle 9.[250] With regard to principle 12, we have recommended in chapter 3 that a new exception for statistical and research uses should be added to principle 12(2). We have not recommended any other exceptions to this principle, but we think there could be cases where an agency might want to make a one-off use of a unique identifier that would be in breach of principle 12 but that would be in the public interest or would involve a clear benefit to an individual.

4.56 One other issue concerning section 54 that was raised in submissions is transparency about exemptions sought or granted. OPC noted that there are transparency requirements associated with codes of practice, but no such requirements for section 54 exemptions. While it is appropriate that the process for one-off exemptions should be less elaborate than that for codes, OPC submitted, there should perhaps be minimum transparency requirements such as public notification or the creation of a public register. If there were to be a

249 Issues Paper at 289–290.

250 Office of the Privacy Commissioner *Review of the Privacy Act 1993: Discussion Paper No 4: Codes of Practice and Exemptions* (Wellington, 1997) at 7–8; *Necessary and Desirable* at 219–220 (recommendation 79).

new public notification requirement, OPC considered that it should be imposed on applicants for exemptions, and that the Privacy Commissioner could perhaps be given a power to waive the requirement in appropriate cases. The Law Commission agrees that the Act should provide for transparency in relation to section 54 exemptions, but we think that the obligation to publish information about such exemptions should rest with OPC rather than with the agency making the application. Notification on an agency's website is unlikely to attract much notice, and a requirement to directly contact affected clients or customers is likely to be disproportionate to the interference with privacy involved in many cases. It is also useful to have a comprehensive report on section 54 exemptions, and OPC is best placed to provide this. While OPC currently reports on section 54 exemptions in its annual report, there is no obligation to do so in the Act. We recommend that the Act should provide that OPC must report annually on exemptions applied for and granted under section 54, and that it must maintain a list of all current exemptions on its website.

RECOMMENDATION

R40 Section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principles 9 and 12.

RECOMMENDATION

R41 Section 54 should be amended to require the Privacy Commissioner to report annually on exemptions applied for and granted under section 54, and to maintain on the Commissioner's website a list of all current exemptions.

Section 55 – exemption of certain information from principles 6 and 7

4.57 Section 55 provides that nothing in principles 6 and 7 (the access and correction principles) applies in respect of certain specified information. We had no proposals for the reform of section 55 in our issues paper, and received no suggestions for amendments to this section in submissions. However, there is one issue raised in a submission that we consider is best dealt with by an amendment to section 55.

4.58 The Office of the Auditor-General (OAG) asked in its submission to be excluded from the coverage of the Privacy Act, except in relation to information about the Office's staff. Further discussion with OAG has established that the Office's concerns are in fact limited to principles 6 and 7. In its submission, OAG explained that audit work involves considering risks and asking questions about the behaviour of individuals, which can be quite sensitive and personal. Auditors need to maintain trust with key management and staff in an entity that they are auditing, and those working for the entity will not discuss matters freely and frankly if they believe those discussions will be disclosed. OAG also receives several hundred requests each year for the Office to inquire into matters of concern, and such requests often contain allegations about the conduct of individuals. OAG protects the identity of those who raise such concerns, and if it contacts the individual or entity to which the concerns relate, it often does not reveal in any detail what was contained in the complaint (both to protect the

identity of the source of the information, and because the information may not be accurate). If OAG decides to undertake an inquiry, it will gather further information, and again much of this may relate to particular individuals. Auditors have an ethical obligation to maintain confidentiality, and are also required by their professional standards to document their investigations extensively. The requirement for documentation includes keeping a record of conversations with individuals, and recording material that, in other contexts, might be considered mere gossip or speculation.

4.59 OAG noted that the confidential nature of their work is recognised by the fact that the OIA does not apply to the Auditor-General. The Public Audit Act 2001 does not include a provision requiring the Auditor-General and his or her staff to maintain secrecy. Section 30 of the Public Audit Act provides that the Auditor-General *may* disclose such information as he or she considers appropriate in the exercise of his or her functions, but before doing so the Auditor-General must consider the public interest, an auditor's professional obligations concerning confidentiality, and certain grounds for withholding information under the OIA. This section expressly states that it does not affect an individual's access rights under the Privacy Act.

4.60 OAG said that it is difficult to reconcile the rights of access under the Privacy Act with the type of work the Office does and the professional obligations of auditors. They gave examples of difficulties they have faced in dealing with access requests:

- A person who is the subject of a complaint seeks access to it, and the information cannot be released without disclosing the source of the information or the fact that an investigation is under way. OAG's submission made clear that their inquiry process protects natural justice by giving individuals who are the subject of inquiries an opportunity to understand the nature of the concerns raised about them, to comment on any information on which OAG proposes to rely, and to provide information to the inquiry. OAG said, however, that difficulties can be created by access requests made at an early stage in the inquiry process.
- An individual wants to know what information OAG holds on its working files about him or her. If any such information exists, releasing it would conflict with the auditor's ethical obligation to maintain confidentiality.

In such cases, OAG sometimes relies on the "maintenance of the law" ground for refusing access.[251] This ground is relevant if there is an investigation under way into possible fraud or other criminal activity, but its applicability is less clear in other cases.

4.61 We are persuaded that OAG faces real difficulties as a result of the application to the Office of the access principle, and we agree that relying on the "maintenance of the law" withholding ground is unsatisfactory. Although the concerns raised with us related to access rights, we can also see that the closely-related right of correction could create very similar problems for OAG. We believe that the best way of dealing with the problems encountered by OAG is to add a new provision to section 55. This new provision would state that principles 6 and 7 do not

251 Privacy Act 1993, s 27(1)(c).

apply in respect of information held by or on behalf of the Auditor-General, and in connection with the Auditor-General's statutory functions. The new provision should also make clear that principles 6 and 7 still apply to personal information relating to the Auditor-General's current, former and prospective staff.

RECOMMENDATION

R42 Section 55 should be amended to provide that principles 6 and 7 do not apply in respect of personal information held by or on behalf of the Auditor-General, and in connection with the Auditor-General's statutory functions. The provision should make clear that principles 6 and 7 still apply to personal information about the Auditor-General's current, former and prospective staff.

Section 56 – personal, family, or household affairs

4.62 Section 56 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.

Similar exemptions are contained in information privacy statutes in other jurisdictions. The rationale behind the exemption is fairly clear: 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.

Definitional issues

4.63 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:[252]

> [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.

252 *S v P* Complaints Review Tribunal 3/98, 12 March 1998 at 4.

4.64 Professor Paul Roth has argued that it is not absolutely clear on the face of the provision that it applies to disclosures,[253] and it was suggested at a meeting organised for us by InternetNZ that this issue should be clarified in the statute. We agree that section 56 should be amended to state expressly that the exemption applies to all of principles 1 to 11. This would make it clear that section 56 applies to the use and disclosure principles, as well as to most of the other principles. We do not think the exemption is relevant to principle 12.

4.65 Paul Roth has also raised questions about the meaning of "personal affairs" in section 56,[254] and we asked in the issues paper whether this term should be clarified. A few submitters said that it should. One suggestion was to contrast personal affairs with other activities, such as business or professional affairs. Another was to incorporate an objective standard by referring to personal information that is of a type that is "ordinarily" collected or held in connection with personal, family or household affairs. In the absence of a strong call in submissions for clarification, or of clear evidence that the term "personal affairs" is currently causing problems, we are not persuaded that any clarification is needed.

Narrowing the scope of section 56

4.66 An exemption like that in section 56 is clearly needed for reasons given above, but it does create a significant gap in the protection afforded by the Privacy Act. This gap has arguably become more problematic with the development of the internet. The question is whether this gap in coverage can be narrowed somewhat without compromising the objectives that the exemption serves.

4.67 Two relatively straightforward recommendations of the Privacy Commissioner, which we supported in our issues paper, are to amend section 56 so that it does not apply where:[255]

- 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); or
- personal information is obtained unlawfully (whether or not the person obtaining the information has been charged with or convicted of a criminal offence).

The second of these proposals has been seen as particularly useful in providing a civil remedy for intimate covert filming.[256] Both proposals were supported by a significant number of submitters, and no submitters opposed the proposals. We recommend that they should be implemented. The recommendation with regard to information obtained unlawfully should cover the collection of personal information by unlawful means, and the use and disclosure of information obtained by unlawful means. This would effectively mean that section 56 does

253 Paul Roth *Privacy Law and Practice* (looseleaf ed, LexisNexis) at [PVA56.4].

254 Ibid, at [PVA56.5].

255 Issues Paper at 137–138.

256 See Law Commission *Intimate Covert Filming* (NZLC SP15, 2004) at 37. As a result of the Law Commission's recommendations on intimate covert filming, such filming has been made a criminal offence: Crimes Act 1961, s 216H.

not provide an exemption from principle 4(a), and this fact could be stated expressly if it is considered that there may be any uncertainty about the application of this principle.

4.68 There are other situations in which, while the potential use of the section 56 exemption is problematic, it is not so clear how or even if the scope of the exemption should be narrowed. We gave some examples in the issues paper.[257] One example concerns a situation in which two people have been in a sexual relationship, in the course of which one takes intimate photographs of the other with consent. When the relationship breaks up, the person who has taken the photographs posts them on a publicly-accessible website *without* the other person's consent. Unfortunately, it seems that this is not an unlikely scenario: on the contrary, the internet safety organisation Netsafe receives fairly frequent calls from people distressed by such incidents.[258] If an individual complained to the Privacy Commissioner about such a disclosure of intimate photos, the person who posted the photos could argue that the privacy principles do not apply because the photos were collected and held in connection with that person's personal, family, or household affairs.

4.69 The issues concerning section 56 do not result only from the development of the internet, but the internet does create new problems when information about personal, family or household affairs is made available to a much wider audience. It could be argued that making the information more widely available via the internet takes it out of the domestic sphere. However, this is by no means clear: increasingly, websites are becoming the modern equivalents of diaries or family photo albums.

4.70 We put forward several options in the issues paper for restricting the scope of the section 56 exemption:[259]

- The wording of the section could be modified so that it is more tightly confined to information collected or held *only* for personal, family or household purposes, rather than "solely *or principally*" as at present.
- Section 56 could provide that the exemption does not apply in certain instances. We gave a number of examples of circumstances in which the Act could provide that section 56 does not apply, but our preferred option was to amend section 56 so that it does not apply when the collection, use or disclosure of personal information results in identifiable harm to another individual.
- The exemption could be removed altogether, but the Act could provide instead that, in dealing with complaints against individuals, the Commissioner and the Tribunal must give due weight to the fact that the information in question was collected or held in connection with an individual's personal, family or household affairs.

257 Issues Paper at 138. See also some examples involving surveillance from the issues paper for stage 3 of this Review: Law Commission *Invasion of Privacy*, above n 229, at 224–234 (see scenarios 1–4, 12, 15).

258 See "Naked Photo Sends Jilted Lover to Jail" *Dominion Post* (Wellington, 13 November 2010) < www.stuff.co.nz > ; Chris Barton "Facebook Shows its Ugly Side" *New Zealand Herald* (Auckland, 20 November 2010) < www.nzherald.co.nz > .

259 Issues Paper at 138–140.

4.71 There was some support in submissions for the first two options, and none for the third. Gehan Gunasekara from Auckland University supported the first option but not the second. Repeating views previously expressed in a journal article,[260] he said that the function of section 56 is to leave a fairly wide social space for individuals to interact outside the scope of information privacy law. OPC, while not opposing any of the options, expressed some caution. It referred to the importance of providing a degree of certainty and clarity, and to the importance of not losing the basic objective of the exemption. That objective, in OPC's view, is to keep the law out of "minor matters that can best be sorted out between individuals living in the same household", and to ensure that the law is not applied in circumstances where its application would be seen as inappropriate by many people.

4.72 We think that section 56 serves an important purpose, and we agree with OPC that any changes to the section should not undermine the section's objective. However, we also think there are some cases in which the collection, use or disclosure of personal information by individuals in connection with their personal, family or household affairs will be so offensive that the exemption should not apply.

4.73 We recommend firstly that the exemption should apply to information collected or held *solely* (not solely or principally) in connection with personal, family or household affairs. This should help to make it clear that a person cannot rely on section 56 when he or she has a secondary purpose unrelated to domestic affairs (such as commercial gain) for collecting or holding the information.

4.74 Second, we recommend that section 56 should not apply to a collection, use or disclosure of personal information that would be highly offensive to an objective reasonable person. This is a change from our proposal in the issues paper that section 56 would not apply when the collection, use or disclosure would result in identifiable harm to another individual. That proposal was made in the context of another proposal, to remove the harm threshold for complaints under the Privacy Act. For reasons set out in chapter 6, we are not recommending in this report that the harm threshold for complaints should be removed. Thus, a reference to harm in section 56 would impose a sort of double harm threshold: actual or potential harm would have to be shown to overcome the section 56 exemption, and then again to ground a complaint. This does not seem to us to be workable.

4.75 Instead, we propose to introduce a "highly offensive" test based on that used in the tort of invasion of privacy. This test, which is also used in the privacy principles of the Broadcasting Standards Authority, would involve a qualitative assessment of the nature of the personal information and the way in which it is collected, used or disclosed. Such an assessment would depart somewhat from the general approach of the Privacy Act, which does not distinguish between different types of personal information on the basis of their sensitivity. In the privacy tort case of *Hosking v Runting*, the Court of Appeal said that "highly offensive" publicity would involve "very personal and private matters", and would be "determined objectively, by reference to its extent and nature, to be offensive by causing real hurt or harm."[261] We think that such a test is appropriate in the context of section 56.

260 Gehan Gunasekara and Alan Toy "'MySpace' or Public Space: The Relevance of Data Protection Laws to Online Social Networking" (2008) 23 NZULR 191 at 213.

261 *Hosking v Runting* [2005] 1 NZLR 1 at [125]–[126].

The threshold it sets is quite a high one, and therefore it will not unduly limit the scope of the domestic affairs exemption, but will provide some recourse in the most offensive instances of misuse of personal information by individuals in connection with personal, family or household affairs.

RECOMMENDATION

R43 Section 56 should be amended to state expressly that the exemption applies to all of principles 1 to 11.

RECOMMENDATION

R44 Section 56 should be amended to provide that it applies to information collected or held "solely" (rather than "solely or principally") for the purposes of, or in connection with, personal, family, or household affairs.

RECOMMENDATION

R45 Section 56 should be amended to provide that it does not apply where:

- an individual 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);
- personal information is obtained unlawfully (whether or not the individual obtaining the information has been charged with or convicted of a criminal offence) – this includes the collection of information by unlawful means, and the use or disclosure of information obtained by unlawful means; or
- the collection, use or disclosure of personal information would be highly offensive to an objective reasonable person.

Section 57 – intelligence organisations

4.76 Section 57 provides that principles 1 to 5 and 8 to 11 do not apply to information collected, obtained, held, used or disclosed by, or disclosed to, an intelligence organisation. Thus, only the access, correction and unique identifier principles apply to these organisations. "Intelligence organisation" is defined in section 2 of the Act as meaning the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB).

4.77 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:[262]

262 New Zealand Security Intelligence Service "Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS" (2009) at [8]–[12] < www.nzsis.govt.nz > [NZSIS "Application"].

- 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. 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.

4.78 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 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. In 2008–2009, 11 complaints concerning the NZSIS were made to the Privacy Commissioner.[263]

4.79 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.[264] 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.

263 New Zealand Security Intelligence Service *Annual Report for the Year Ended 30 June 2009* (2009) at 18.

264 Inspector-General of Intelligence and Security Act 1996, s 11(1)(a) and (b).

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.[265]

Extending other privacy principles to the intelligence organisations

4.80 The Privacy Commissioner recommended in *Necessary and Desirable* that section 57 should be amended to provide that privacy principles 1, 5, 8 and 9 would apply to the intelligence organisations, in addition to those principles that already apply to them.[266] The Commissioner argued that these principles "provide a sound basis for fair information handling and have clear relevance to intelligence organisations".[267] We asked about this recommendation in our issues paper, and there was general support for it. The intelligence organisations stated in their submissions that they had no objections to becoming subject to principles 1, 5, 8 and 9. The two organisations did, however, have a caveat with regard to principle 9. They noted that they often need to retain information for long periods even when they cannot be sure of its future relevance, and that some recognition of their special position with respect to principle 9 was needed.[268] It does not appear that they were asking for any special provisions in the Act in relation to principle 9, but simply for flexibility in the way in which they apply it. In light of these submissions, and of the general principle that all exemptions in the Act should be as limited as possible, we recommend that principles 1, 5, 8 and 9 should apply to the intelligence organisations.

Complaints processes

4.81 We asked in the issues paper whether there should be any changes to the procedures for investigating privacy complaints involving the intelligence organisations, and whether the dual jurisdictions of the Privacy Commissioner and the Inspector-General of Intelligence and Security create any problems. The two oversight bodies (Privacy Commissioner and Inspector-General) reported no problems with their overlapping jurisdictions. Likewise, the NZSIS favoured retaining the jurisdiction of the Privacy Commissioner to investigate complaints alongside that of the Inspector-General (and of the Chief Ombudsman with respect to OIA issues). They saw this oversight as important from the point of view of public trust. The GCSB expressed a preference for the Inspector-General to be the oversight body for the intelligence organisations with respect to compliance with the privacy principles. However, the Bureau also said that they have experienced no problems with the dual jurisdiction, and that they are the subject of few if any privacy complaints. We recommend no change to the complaints provisions relating to the intelligence organisations.

265 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.

266 *Necessary and Desirable* at 224–229 (recommendation 83).

267 Ibid, at 226.

268 There is some useful discussion of information retention issues in a report of the Inspector-General of Intelligence and Security to the Prime Minister concerning NZSIS records, 28 April 2010, available on the NZSIS website < www.nzsis.govt.nz > .

Access requests and "neither confirm nor deny"

4.82 The intelligence organisations are subject to rights of access under principle 6. Recently there has been a large increase in the number of access requests received by the NZSIS, probably as a result of media publicity about some access requests involving politicians and political activists. There were only 10 Privacy Act requests to the NZSIS in 2007, but 303 in 2009.[269]

4.83 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.

4.84 The NZSIS often relies on the ability to neither confirm nor deny under section 32, and has set out its reasons for doing so.[270] 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."[271] 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. In particular, it states that:[272]

- 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.

4.85 In its submission, the NZSIS explained further that the Service is particularly concerned about "orchestrated requests", in which two or more people working together make access requests. If Person A receives a "neither confirm nor deny" response and Person B receives a "no information held" response, this could be seen as an indication that Person A is of interest to the NZSIS. As a result, the NZSIS said, the only option for it is to use the "neither confirm nor deny" response more broadly than it would wish. The NZSIS proposed in its submission that the most appropriate solution would be to provide it with a partial exemption from the access principle. This exemption would be limited to intelligence investigatory material (as opposed, for example, to material relating to security

269 Ibid, at [11].

270 NZSIS "Application", above n 262, at [13]–[18].

271 Ibid, at [14].

272 Ibid, at [19].

clearance applications) held by intelligence organisations, and could be limited to material created within a particular period (such as within 25 years of the request). Any such exemption, the NZSIS submitted, would need to be accompanied by robust accountability mechanisms, such as annual reporting and powers for the Privacy Commissioner to review the application of the exemption.

4.86 The proposal put forward by the NZSIS involves a significant change to the existing provisions relating to the intelligence organisations, and we have not had submissions on the proposal from other interested parties. We think it is best considered in the context of a wider review of the legislative framework governing the NZSIS (and perhaps also the GCSB), and that any change could be implemented through an amendment to the New Zealand Security Intelligence Service Act 1969, rather than to the Privacy Act. A fundamental review of the NZSIS Act has been proposed during the next two or three years,[273] and we think that would be an appropriate place in which to consider the issues raised by the NZSIS with regard to Privacy Act access requests. In the meantime, the NZSIS can continue to use the "neither confirm nor deny" provisions in section 32 of the Privacy Act, and we note that the Service's use of section 32 has been supported in a recent Privacy Commissioner case note.[274]

RECOMMENDATION

R46 Section 57 should be amended to provide that principles 1, 5, 8 and 9 apply to the intelligence organisations, in addition to principles 6, 7 and 12 as at present.

NEW EXCLUSIONS AND EXEMPTIONS

4.87 We do not think that any new exclusions or exemptions are needed in the Privacy Act, apart from the new provision relating to the Office of the Auditor-General in section 55, as discussed above.

273 "Regulatory Impact Statement: Modernising NZSIS Legislation – High Priority Amendments" (2010) at [29], [33], available at < www.nzsis.govt.nz > .

274 *An Individual Requests Personal Information from the New Zealand Security Intelligence Service* [2010] NZ PrivCmr 25, Case Note 219773.

Chapter 5

Role, functions and powers of the Privacy Commissioner

5.1 In this chapter we review the Privacy Commissioner's existing role, functions and powers, explain how they work in practice and present recommendations for reform. This chapter also covers the issuing of codes of practice under Part 6 of the Privacy Act.

OVERVIEW

5.2 The Commissioner has extensive functions under the Privacy Act and also 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

5.3 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(1) of the Act:

> 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:

(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.

Functions and powers elsewhere in the Privacy Act

5.4 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 are in fact not specifically listed in section 13. They include the power to:

- refer to the Director of Human Rights Proceedings the question of whether proceedings for a declaration should be commenced;[275]
- publish directories of personal information;[276]
- authorise a public sector agency to charge for access to and correction of personal information;[277]
- inquire into a public register provision;[278]
- issue codes of practice that modify the application of the privacy principles in relation to a particular type of information, agency, activity or industry;[279]
- exempt an agency in a particular case from principles 2, 10 or 11;[280] and
- receive and investigate complaints.[281]

The Commissioner also has the function of reviewing the operation of the Privacy Act every five years,[282] and powers and functions in relation to information matching.[283]

5.5 It will be seen that some of these "other" functions are among the most important that the Commissioner possesses. In particular, the complaints jurisdiction, the power to make codes and the information matching jurisdiction go to the very heart of the Commissioner's raison d'être.

275 Privacy Act 1993, s 20.

276 Privacy Act 1993, s 21. This effectively repeats a function also listed in s 13: see s 13(1)(d).

277 Privacy Act 1993, s 36.

278 Privacy Act 1993, s 61.

279 Privacy Act 1993, Part 6. See further discussion of the Commissioner's code-making power below.

280 Privacy Act 1993, s 54.

281 Privacy Act 1993, Part 8. See ch 6 below.

282 Privacy Act 1993, s 26.

283 Privacy Act 1993, Part 10. See Issues Paper, ch 9, and appendix 2 of this report

Functions under other enactments

5.6 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 complaint-handling function. These functions can be broadly divided into the following categories:

- complaints investigation;[284]
- scrutiny or approval of information disclosure arrangements;[285]
- consultations with the Commissioner by other agencies (including referral of complaints from other agencies);[286]
- appointment to other bodies;[287]
- codes of practice;[288]
- information matching;[289] and
- advice on privacy impact assessments.[290]

Exercise of the functions

5.7 As we have outlined above, the Commissioner has many functions, and these functions are diverse in nature. Consequently, the Office of the Privacy Commissioner (OPC) carries a heavy workload. For example, in addition to pursuing upwards of 800 complaints a year, it runs around 70 training programmes, handles about 6,000 calls on its inquiries line, and is consulted on over 250 policy and legislative developments each year. A fuller account of its activities is contained in our issues paper.[291]

5.8 Some of the Commissioner's statutory functions have never been exercised. They include the power to audit an agency:[292] this has not been exercised simply because no agency has ever asked to be audited. There is no directory of personal information.[293] The power to report to the Prime Minister[294] has not been needed to date, although the Office views this as a "reserve power" that is useful in securing voluntary compliance with the Act.

---

284 Health Act 1956, s 22F; Domestic Violence Act 1995, ss 118–120 and Domestic Violence (Public Registers) Regulations 1998, reg 11; Social Security Act 1964, s 11B.

285 Passports Act 1992, s 36; Customs and Excise Act 1996, s 281.

286 Official Information Act 1982, s 29B; Local Government Official Information and Meetings Act 1987, s 29A; Health and Disability Commissioner Act 1994, ss 23 and 36; 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.

287 Currently none. Formerly Human Rights Act 1993, s 7.

288 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).

289 Social Security Act 1964, s 11A; Education Act 1989, ss 226A and 238B.

290 Immigration Act 2009, s 32.

291 Issues Paper at [6.19]–[6.44].

292 Privacy Act 1993, s 13(1)(b).

293 Privacy Act 1993, s 21.

294 Privacy Act 1993, s 13(1)(c), (p), (q), (r).

PROPOSALS FOR REFORM OF THE COMMISSIONER'S FUNCTIONS

5.9 We proceed now to discuss whether, and if so to what extent, the current functions of the Privacy Commissioner should be reformed.

The wording of section 13

5.10 The title to section 13 is "Functions of Commissioner". Section 13(1) begins: "The functions of the Commissioner shall be …". Although section 13(1)(u) does refer to the functions conferred by other provisions, it is too easy for an unpractised reader to assume that the itemised list of paragraphs in section 13(1) is, if not an exhaustive list of the Commissioner's functions, then at least a list of the Commissioner's main functions. That is very far from being the case, as we have seen. The Commissioner's core functions are contained elsewhere. We think it would be clearer if section 13 was headed "Additional Functions of Commissioner", and if its introductory words expressly stated that the functions listed in the section are *in addition* to the functions provided for elsewhere, both in the Privacy Act and other legislation.

RECOMMENDATION

R47 Section 13 should be amended to make it clear that it is not a complete list of the Privacy Commissioner's functions.

The breadth of the Commissioner's functions

5.11 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. Indeed, a good number of the paragraphs in section 13(1) refer simply to matters affecting "the privacy of the individual".[295] 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 to privacy of personal information.[296] It had a "watchdog" role which has now been inherited by the Privacy Commissioner.

5.12 In the issues paper we asked whether the Commissioner's role should be confined to *information* privacy on the ground that this would align better with the scheme of the Act. We also noted the difficulty of defining "privacy", and said:[297]

> 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.

295 See Privacy Act 1993, s 13(1)(g) – (k) and (m) – (r).

296 Human Rights Commission Act 1977, Part 5.

297 Issues Paper at [6.48].

5.13 We noted, on the other hand, that it could be artificial to split the various aspects of privacy, and said that it could cause practical difficulties in determining what is, and what is not, within the proper scope of the Commissioner's role.[298] Moreover, in our report on stage 3 of the Privacy Review, we recommended that the Commissioner have extended functions in relation to monitoring surveillance.[299] With the rapid growth of technology it is becoming increasingly important that someone have a watching brief over its privacy-invasive tendencies. If the Privacy Commissioner is not to perform these monitoring functions, who else would do it?

5.14 No submitters to our issues paper thought that the Privacy Commissioner's functions should be confined to protecting personal information. They preferred the concept of an independent body with a wide jurisdiction. We therefore do not recommend any confinement of the Privacy Commissioner's functions.

Should any functions be removed?

5.15 We believe that sections 13(1)(d) and 21 of the Act, which empower the Privacy Commissioner to publish directories of personal information, should be deleted. The apparent objective of these provisions is to assist members of the public to know where personal information is located, and thus more effectively to exercise their rights under the Act. However, OPC has found that maintaining such a directory presents significant practical difficulties, including resource constraints on the Office and compliance costs on agencies.

5.16 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.[300] Most submitters to the issues paper agreed with this proposal, and we so recommend.

5.17 The directory was meant to be one step in complying with the OECD openness principle. In chapter 3 we consider whether an openness principle should be included in the Act.

RECOMMENDATION

R48 Section 13(1)(d) and section 21 should be repealed.

298 Issues Paper at [6.50].

299 Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, 2010) at [R18].

300 *Necessary and Desirable* at [3.11] (recommendation 40).

Should any functions be amended?

Review of the Act

5.18 Section 26 requires the Privacy Commissioner to review the operation of the Privacy Act every five years. It is not common for Acts to "build in" a statutory review requirement, although there are other examples.[301] We wondered, now that the Act is 18 years old, whether the periodic review requirement should continue. We conclude that it should. The Privacy Act operates in an environment that changes more rapidly than most. Technology has become the most potent threat to privacy, and it is developing at lightning speed. International developments also move quickly; information is an international commodity. The Act needs to keep pace. We therefore support a continuing requirement of review.

5.19 The next question is who should undertake the review. From one perspective the Privacy Commissioner may be seen as the appropriate reviewing authority. Privacy is a far more complex matter than many realise, with an international as well as a national dimension. The Commissioner has the appropriate expertise, and is fully abreast of international developments. But there is a danger of the perception that that solution might create. The Privacy Commissioner might be seen as insufficiently impartial and objective, given that the subject matter of the review would directly involve his or her role. Regardless of whether such a perception were justified, it might detrimentally affect public confidence. It was in fact noted in *Necessary and Desirable*, the report of first periodic review of the Act by the then Privacy Commissioner, that just such criticism was voiced at the time.[302] Moreover, individuals and organisations who deal with OPC are likely to be more frank in sharing their concerns about the operation of the Act with an independent reviewer rather than with OPC, particularly if they have negative feedback about the Office.

5.20 A further reason is that if it is necessary to recommend enhancement of OPC's powers, such recommendations carry more weight if they come from a perceptibly independent source.

5.21 On balance, we believe it would be best if the Act were to be reviewed by an independent person or agency. The majority of submitters to the issues paper agreed. We so recommend.

5.22 Various views were put forward as to who the independent reviewer should be. Suggestions included the Ombudsmen, the Law Commission and the Ministry of Justice. We would prefer the Act simply to specify that the Minister should appoint a review committee, which should contain persons expert in privacy, law and technology. It goes without saying that this committee would be expected to consult with the Privacy Commissioner.

301 See for example Evidence Act 2006, s 202.

302 *Necessary and Desirable* at [3.16.3]–[3.16.9].

5.23 There was also a question as to whether five years is an appropriate interval between reviews. It might be thought that, now that the Act has "bedded in", a longer period, say 10 years, might be appropriate. There was a division among submitters on this point. Given the speed at which technology is moving, with consequent threats to privacy, we feel that five years is about right. We did not think the arguments for changing that time span were compelling.

5.24 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. The Commissioner has previously noted difficulties in the implementation of 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 on 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.[303] We support that. The requirement could be introduced through amending section 26, or by a Cabinet circular. Nine out of 10 who made submissions on this topic agreed. No doubt in formulating its response the Government would seek the views of the Privacy Commissioner.

RECOMMENDATION

R49 The Privacy Act should contain a provision that it is to be reviewed every five years. The review should be undertaken by a committee appointed by the Minister, and containing persons expert in privacy, law and technology.

RECOMMENDATION

R50 The Government should be required to table in Parliament within six months a response to each review of the Act.

Reports to the Prime Minister

5.25 Section 13(1) currently contains a number of paragraphs empowering reports to the Prime Minister.[304] These powers to report matters to the Prime Minister have never been exercised. Even if power to report on these matters is desirable, we wondered whether reports need to be to the Prime Minister as opposed to the portfolio minister. We asked about this in our issues paper. Not many submitters answered this question, and among the few who did, responses were evenly divided. Those who supported retention of the power to report to the Prime Minister thought it was a "useful fall-back", particularly in recommending such matters as ratification of international conventions. OPC thought that the mere existence of such a power can encourage cooperation from agencies, and also demonstrates to the international community that OPC is an independent body which can raise issues at the highest level.

303 *4th Supplement to Necessary and Desirable* at recommendation 46A.

304 Privacy Act 1993, s 13(1)(c), (p), (q) and (r).

5.26 The power is unusual. Most other independent Crown entities do not have it: they report directly to their portfolio minister. Nevertheless we have concluded that we should not disturb the present position. There is no demonstrable need to do so. In addition to the reasons for the existence of the reporting power already given, we note two others. One is that the Privacy Commissioner has a role which spans the whole of government (and indeed the private sector too). It may at times be necessary to report a concern which transcends individual ministers' portfolios. The other is that the Privacy Commissioner deals with what is really a human rights issue. The other Commissions which have a "human rights" jurisdiction can also report directly to the Prime Minister: the Children's Commissioner[305] and the Human Rights Commission.[306] We therefore believe it is appropriate to retain the current reporting power as it is, unusual though it may be.

Should the functions be consolidated?

5.27 We are struck by the length of the list of functions in section 13(1). Some of them seem to be repetitive, or at least to overlap: paragraphs (a) and (g), and (f) and (o), for instance. In the first privacy review, the then Privacy Commissioner concluded that each paragraph served a purpose, and thought the detailed specification ensured that the Commissioner does not exceed his or her statutory remit.[307]

5.28 However, everyone who addressed this issue in submissions to our issues paper thought that the list could be consolidated with advantage. OPC did not oppose this, and indeed put forward a suggested redraft should we decide to move to consolidate. That draft is as follows:

> The functions of the Commissioner are –
>
> (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 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:

305 Children's Commissioner Act 2003, s 12(1)(k).

306 Human Rights Act 1993, s 5(2)(k).

307 *Necessary and Desirable* at [3.3.1].

(e) to make public statements in relation to any matter affecting the privacy of the individual or of any class of individuals:

(f) to receive and invite representations from members of the public on any matter affecting the privacy of the individual:

(g) to consult and co-operate with other persons and bodies concerned with the privacy of the individual:

(h) 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 including to provide advice (with or without a request) to a Minister or an agency on any matter relevant to the operation of this Act:

(i) 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:

(j) 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:

(k) 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:

(l) 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:

(m) 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.

5.29 This is still long, but we think it is a great improvement. It reduces 21 paragraphs to 13. We recommend its adoption (subject to any amendments to particular functions which may arise from this report).

RECOMMENDATION

R51 The list of the Privacy Commissioner's functions in the present section 13 should be abridged and consolidated as set out in paragraph (b).

CODES OF PRACTICE

5.30 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 allow for greater specificity, by providing a mechanism through which the specific needs and circumstances of particular agencies, businesses, industries, or professions can be accommodated.

The existing framework

5.31 Part 6 of the Act empowers the Privacy Commissioner to issue codes of practice. 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.[308] A code of practice may:[309]

- 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.

5.32 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.

5.33 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.[310]

308 Privacy Act 1993, s 46(3).

309 Privacy Act 1993, s 46.

310 Privacy Act 1993, s 53(a) and (b).

5.34 The Privacy Commissioner can issue a code of practice on his or her own initiative, or on application by someone else.[311] In the latter case, 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.

5.35 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.[312] 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.[313] 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.[314]

5.36 The code of practice development process is therefore lengthy and relatively complex. The consultation requirements are a significant part of the process.[315] However, there is provision for the issuing of urgent codes when necessary. Urgent codes do not need to go through the usual consultation process, but must be issued on a temporary basis, and must remain in force for no longer than one year.[316]

5.37 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.[317] A code cannot come into force earlier than the 28th day after its notification in the *Gazette*.[318]

5.38 Codes of practice are a form of delegated legislation known as "deemed regulations". They are prepared and issued by the Commissioner. They do not go through the process of being prepared by departments, drafted by Parliamentary Counsel Office and made by the Governor-General in Council. The Acts and Regulations Publication Act 1989 does not apply to them, and they are not published in the Statutory Regulations series. 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.[319]

---

311 Privacy Act 1993, s 47(1).

312 Privacy Act 1993, s 48(1)(a).

313 Privacy Act 1993, s 48(1)(b).

314 Privacy Act 1993, s 51(2).

315 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.

316 Privacy Act 1993, s 52. The Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) was issued using the Commissioner's power to issue an urgent code.

317 Privacy Act 1993, s 49(1).

318 Privacy Act 1993, s 49(2).

319 Privacy Act 1993, s 50. For further information on deemed regulations, see Parliamentary Counsel Office "What are deemed regulations?" < www.pco.parliament.govt.nz/what-are-deemed-regulations > .

Current codes

5.39 There are three main codes of practice currently in force. These are as follows:

- Health Information Privacy Code 1994;
- Telecommunications Information Privacy Code 2003; and
- Credit Reporting Privacy Code 2004.

We explain the detail of each of these codes in our issues paper.[320] There are also 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.[321] In addition, a temporary code was issued in 2011 to facilitate information sharing in the wake of the Christchurch earthquake.[322] To date, three codes have been revoked or have expired.

5.40 As we stated in the issues paper, we have not reviewed the content of individual codes as part of this Review; that is a matter for the Privacy Commissioner.

A comparison with overseas approaches[323]

5.41 In Australia, by virtue of the Privacy Act 1988 (Cth), as amended in 2000, codes which are developed by organisations and approved by the Privacy Commissioner take the place of the National Privacy Principles for those organisations. But, significantly, 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. Moreover, 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.

5.42 In its recent review of the Privacy Act 1988 (Cth), the ALRC considered that privacy codes under that Act 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.[324] 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.[325] The ALRC did not recommend that the Privacy Commissioner should have power to issue binding codes, despite strong support among stakeholders.[326] 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.[327]

320 Issues Paper at [7.11]–[7.38].

321 Superannuation Schemes Unique Identifier Code 1995 and Justice Sector Unique Identifier Code 1998.

322 Christchurch Earthquake (Information Sharing) Code 2011 (Temporary).

323 The overseas jurisdictions are examined in more detail in Issues Paper at [7.39]–[7.54].

324 *For Your Information* at recommendation 48–1.

325 *Enhancing National Privacy Protection* at 89.

326 *For Your Information* at [48.34].

327 *Enhancing National Privacy Protection* at 89–90.

5.43 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).[328] The responsible Minister can then decide whether or not to make the code.[329] Codes are drafted by the Parliamentary Counsel's Office, made by order of the responsible Minister and published in the *Gazette*.[330] Codes can modify the application of one or more of the information privacy principles as they apply to any particular public sector agency (the Act does not apply to the private sector). Importantly, the Act states that codes may not impose requirements on public sector agencies that are more stringent (or of a higher standard) than the privacy principles require.[331] Agencies to which any particular code applies must comply with its provisions.[332]

5.44 In the United Kingdom, the relevant Act is the Data Protection Act 1998. It provides that the Information Commissioner is to prepare and disseminate appropriate codes of practice for guidance as to good practice. Codes of practice issued under section 51 of that Act do not have the same legal status as codes of practice issued under the New Zealand Privacy Act 1993. 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.

5.45 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, prescribe standards that are more stringent or less stringent, or exempt actions from the privacy principles. Breach of the code is deemed to be breach of a privacy principle. Australian Federal codes cannot prescribe standards that are less stringent 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.

328 Privacy and Personal Information Protection Act 1998 (NSW), Part 3.

329 Privacy and Personal Information Protection Act 1998 (NSW), s 31(4).

330 Privacy and Personal Information Protection Act 1998 (NSW), s 31(5).

331 Privacy and Personal Information Protection Act 1998 (NSW), s 29. However, the New South Wales Law Reform Commission has recommended reversing this position, so that privacy codes of practice could not derogate from the privacy principles but only increase privacy protection or clarify the application of the principles: New South Wales Law Reform Commission *Protecting Privacy in New South Wales* (NSWLRC R127, Sydney, 2010) at 152–155.

332 Privacy and Personal Information Protection Act 1998 (NSW), s 32.

The concept and scope of codes

5.46 Few codes of practice have been issued under the Privacy Act 1993 during the 18 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.[333] This remains the case.

5.47 On this basis, our overall conclusion is that the principles-based approach in the Privacy Act, together with the guidance and advice provided by OPC, is working satisfactorily for most agencies to which the Act applies, without the need for more specific codes of practice.

5.48 Nevertheless, the importance of the code of practice mechanism in the Privacy Act must not be underestimated. The codes that have been issued in New Zealand, while small in number, cover key areas such as the health, credit reporting and telecommunications sectors. The value of a code-making provision as a "reserve power", to be used if other measures fail, is also of significance. 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.

5.49 Subject to what we say below, our research has not uncovered significant problems of substance with the code of practice mechanism in the Privacy Act. It appears to be working satisfactorily, a view shared by OPC. However, the limitations 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 are obvious from the Health Information Privacy Code.[334]

5.50 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.

5.51 We asked in the issues paper whether any changes to the provisions of the Act relating to codes of practice were necessary to improve the effectiveness of codes. There was little mood for change, and we do not recommend any as far as the substance of codes is concerned.[335]

333 *Necessary and Desirable* at [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.

334 See discussion of health in ch 12.

335 However, we do recommend in ch 2 an amendment to the code-making provisions to allow a code to apply any of the privacy principles to information about deceased individuals (R5).

The code-making process

5.52 We have, however, spent much time considering the code-making *process*. Most aspects of that process are necessary and desirable. 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 that independence and expertise to bear in the development of codes of practice. The process of making 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.

5.53 The work involved on the part of OPC in developing and consulting on a code is very extensive for a small organisation, even though OPC is now better resourced than when it was first established. Having considered the submissions to our issues paper, we would not wish to diminish the thoroughness of the present process.

5.54 However on one significant matter we do recommend a change. We consider that more constitutional safeguards should be added to the code-making process.

5.55 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.[336] This sort of power should be granted by Parliament "rarely and with strict controls".[337]

5.56 Moreover, despite these being Henry VIII provisions, codes do not follow the conventional process for regulation-making in New Zealand. 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. The Regulations Review Committee has examined one code of practice and identified issues with it.[338] It was of the view that changes were required, and these were subsequently made to the Committee's satisfaction.

5.57 We nevertheless consider that accountability for the exercise of the 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. We believe that codes of practice should also undergo this process.

336 For more on Henry VIII clauses see Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2001, most recently amended 2007) at 205–206.

337 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.

338 Telecommunications Information Privacy Code, discussed in Issues Paper at [7.25]–[7.30].

5.58 In making this suggestion, we certainly 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 to considerable lengths to ensure that the process of code development is open and transparent, and the final product of a high standard and readily accessible.

Model process

5.59 The sort of model we have in mind is similar to the one incorporated in the Health and Disability Commissioner Act 1994. Under that Act, the Health and Disability Commissioner (H&D Commissioner) is required to develop a Code of Health and Disability Services Consumers' Rights (CHDSCR).[339] Notification and consultation obligations similar to those contained in the Privacy Act apply to the development of a Code by the H&D Commissioner.[340] But while the Commissioner proposes, Cabinet disposes. Once a draft Code has been developed, the H&D Commissioner forwards it to the Minister, who must present it to the House.[341] 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.

5.60 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 H&D Commissioner, or contrary to or without the H&D Commissioner'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 H&D Commissioner, 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.[342]

5.61 This model is not entirely appropriate for codes of practice under the Privacy Act, however. A CHDSCR needs to be in place for the Health and Disability Commissioner Act to work. So the option of prescribing a code that has not been recommended by the H&D Commissioner has to be available to the Executive. Codes of practice are not essential to the operation of the Privacy Act.

5.62 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 Governor-General in Council should be able to reject the proposed code, but not modify it.[343] If the Governor-General in Council rejects the code, the Minister should have to give reasons to the House.

---

339 Health and Disability Commissioner Act 1994, s 19.

340 Health and Disability Commissioner Act 1994, s 23.

341 Health and Disability Commissioner Act 1994, s 19.

342 Health and Disability Commissioner Act 1994, s 75.

343 The House of Representatives could still amend or replace the code, once incorporated in regulations, through the power conferred by s 9 of the Regulations (Disallowance) Act 1989.

5.63 This was the model we proposed in our issues paper. A majority of the submitters agreed with it. However, a minority did not, and suggested a continuation of the status quo. Their reasons can be summarised as follows.

5.64 First, there was a fear that the need for a final Cabinet "sign-off" might derail a proposed code which had already undergone the intensive consultative process required. Industry participants might want to investigate the matter and the Minister might be lobbied; government officials might have ideas of their own at variance with the position arrived at in the consultation process.

5.65 Secondly, we heard some concern that such a new process might jeopardise meaningful participation by industry in the code-development process. The risk that the Executive might disallow a code, after all the work that had gone into it, might discourage engagement from the outset.

5.66 Thirdly, there were concerns that the proposed process would be less flexible and less responsive than the present one. Amendment would be more difficult, and there might be a disinclination to make even small but necessary amendments.

5.67 Fourthly, there was a view that in this delicate area involving personal information it would be unwise to allow government the final say. This would give it more control over an area in which it might be perceived to have a vested interest.

5.68 Yet these considerations are present, to a greater or lesser extent, in many other contexts where traditional regulation-making is the prescribed method. We think it unlikely that a code would be "derailed"; the robustness of the code-development process, and the status of the Privacy Commissioner, make this unlikely. Moreover, the Executive would only be able to reject a code, not amend it, and would have to give reasons publicly for doing so: these are significant safeguards. We acknowledge that the dynamics of negotiating a code may change subtly if it requires Cabinet approval, but we think this would be unlikely to influence the outcome.

5.69 The Legislation Advisory Committee Guidelines[344] make it clear that there needs to be a strong case for departing from the "traditional" way of making delegated legislation. According to the Guidelines, the main matters which can justify such a departure are: that the subject matter is of a technical nature; that the audience is a limited section of the public; that the rules will have only a limited effect on the public; that it is desirable to promote self-regulation; that there are strong policy reasons against government intervention (as in the Broadcasting Codes which are founded in freedom of expression); or that there is a likelihood of a need for urgent change. None of those special reasons obviously exist in the case of privacy codes.

344 Legislation Advisory Committee, above n 336, at [10.4.2].

5.70 Nor would the Privacy Commissioner's statutory independence seem in itself to be a reason:[345] the Health and Disability Commissioner has a similar status, but the Code under that legislation requires Cabinet authorisation.[346] In other analogous areas involving human rights, codes require sign-off by the relevant Minister: examples include Retirement Villages Codes[347] and the International Students Code.[348] It is not apparent why privacy codes should be subject to any fewer checks and balances.

5.71 In the case of the privacy codes there are some striking features which argue strongly in favour of a "traditional" process for delegated legislation. Privacy codes can actually amend an Act of Parliament, a rare and unusual power even in the case of traditional regulations, let alone codes which are not regulations. Moreover they affect, and have important consequences for, the public at large, as is clear from the three main codes currently in existence: those relating to health, telecommunications and credit reporting. Codes can also impose liability on those who fail to comply with them. Non-compliance is ground for a complaint to the Privacy Commissioner, and may result in an award of damages from a judicial tribunal.

5.72 Scrutiny by the Executive in making codes would provide a broader perspective and another set of checks and balances. Without such intervention, the Privacy Commissioner makes the law, interprets it and enforces it.

5.73 Moreover, a code of practice may not always be the most appropriate way of dealing with an issue. It is appropriate that the government of the day have the final say on that. 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. For example, when the question of a national student number was raised, the Ministry of Education noted that a code was not the appropriate vehicle because it does not provide the same opportunity for Parliamentary debate and decision-making as legislation does.[349] 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.

5.74 So it is our conclusion that there is no strong reason why the privacy codes should not be made as traditional regulations, and a number of good reasons why they should be. We therefore support the proposal that we put forward in our issues paper.

---

345 The reference in the LAC Guidelines to "independent statutory function" is illustrated in those guidelines only by the Privacy Act codes: it can hardly be suggested that the status of an independent Crown entity should automatically justify such a law-making power.

346 Health and Disability Commissioner Act 1994, ss 19–23, 74.

347 Retirement Villages Act 2003, s 89; in addition there is a code of residents' rights, the essential content of which is set out in sch 4 of the Act itself.

348 Education Act 1989, s 238F.

349 See Issues Paper at [7.82].

RECOMMENDATION

R52 Codes of practice should continue to be developed by the Privacy Commissioner, but should require approval by the Governor-General in Council.

RECOMMENDATION

R53 The Governor-General in Council should be able to reject a proposed code, but not to amend it. If a code is rejected, the Minister should provide reasons to the House of Representatives.

Time limits on codes

5.75 In our issues paper we considered one further matter: whether codes should be "sunsetted", or at least subject to mandatory review, after a set period of time, say five years. There is a particular reason for suggesting this. 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).[350]

5.76 While section 46 of the Privacy Act states that a code may provide for its review by the Commissioner, and also for its expiry, neither are presently mandatory. We asked in our issues paper whether they should be. A majority of submitters supported a mandatory review after a set period of time. However, OPC (and others) noted the resource implications of mandatory reviews. Sunsetting is no different: it effectively requires a review. In the end we have decided that this resource implication is a strong consideration, and that we should not recommend mandatory reviews or sunset provisions. It should be enough that the Act continues to empower reviews. If a code is not working there will likely be complaints from industry and others, and a review can be initiated as and when required.

5.77 This is not to say, of course, that there may not sometimes be temporary codes which contain express expiry clauses. Indeed, codes issued urgently in accordance with section 52 are required to be temporary. A good example is the Christchurch Earthquake (Information Sharing) Code 2011 which was made to deal with an emergency situation.

350 Regulations Review Committee, above n 337.

Chapter 6

Complaints, enforcement and remedies

6.1 This chapter examines the complaints system under the Privacy Act and considers whether the existing approach needs amendment.

6.2 An important aim of the present Act is to secure voluntary compliance with its principles. In part that is achieved by providing guidance, education and assistance. But voluntary compliance is also an important aim of the complaints system. On receiving a complaint the Privacy Commissioner must attempt to reach a settlement between the parties. If that fails, there is provision for the matter to proceed to an enforcement stage in the Human Rights Review Tribunal ("the Tribunal"). (A simplified flowchart of the process by which complaints can proceed from the Privacy Commissioner's investigation to the Tribunal is set out as Figure 1 at the end of this chapter. Figure 2 shows how the process would change if certain of our recommendations for reform are accepted.) The Act's privacy principles are not enforceable in the courts, with the exception of principle 6, which deals with access to personal information where that information is held by a public sector agency. The Privacy Commissioner does not have power to require compliance: enforcement is not, at present, the Commissioner's role.

OVERVIEW OF THE PRESENT SYSTEM

Complaints to the Privacy Commissioner

6.3 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:[351]

- has caused, or may cause, loss, detriment, damage or injury to the complainant; or

351 Privacy Act 1993, s 66(1)(b).

- 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 Privacy Commissioner's complaints jurisdiction.

6.4 In the 2009–2010 year the Commissioner received 978 complaints, the great majority relating to denial of access to personal information under principle 6 and disclosure of personal information in breach of principle 11.[352]

6.5 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 of the Privacy Commissioner (OPC) 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, and this new methodology has been adopted.

6.6 OPC 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.[353] In 2009–2010, 244 complaints were closed by mediation or settlement, and 123 were withdrawn or not pursued by the complainant.[354] Sometimes during the investigation, investigating officers may indicate a legal view of the complaint to assist one or both of the parties to understand the strength of their case, with a view to encouraging settlement. If settlement does not occur, a more formal legal opinion may be given and a decision made on 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.

6.7 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.[355] In the 2009–2010 year the Commissioner referred 18 complaints to the Director, up from 12 the previous year.[356] Since 2002 the average number of complaints so referred is about 15 a year.

352 Office of the Privacy Commissioner *Annual Report 2010* (Wellington, 2010) at 30–32 [*Annual Report*].

353 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) at 29.

354 Office of the Privacy Commissioner *Annual Report*, above n 352, at 35.

355 Privacy Act 1993, s 77.

356 Office of the Privacy Commissioner *Annual Report*, above n 352, at 40.

Director of Human Rights Proceedings process[357]

6.8 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 information from the Commissioner about the complaint.

6.9 The Director considers the complaint afresh in order to decide whether to begin proceedings in 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.[358] The only requirement is that the Director must give respondents an opportunity to be heard before instituting proceedings against them.[359]

6.10 The current Director bases his practice 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. In many cases, settlement offers are made during this process, and a considerable number of cases are settled at this point.

6.11 After hearing from the parties and considering the facts, the Director then decides whether to bring proceedings. In making this decision, the current 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.

6.12 If the Director decides to take the case, he will then notify the parties and begin proceedings in the Tribunal. Remedies sought could include a declaration of breach, an order preventing further breaches, an order that specific steps be taken to prevent further breaches, compensation and costs. Under the Act the Director acts as the plaintiff, rather than appearing for the complainant.[360]

6.13 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. As noted above, in 2010 the number of privacy cases referred was 18.

357 See generally Robert Hesketh "The Role and Function of the Director of Human Rights Proceedings in Cases under the Privacy Act 1993" (presentation to Privacy Issues Forum, Wellington, 30 March 2006).

358 Privacy Act 1993, s 77(3).

359 Privacy Act 1993, s 82(3).

360 Privacy Act 1993, s 82.

Human Rights Review Tribunal process

6.14 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.[361] In such cases the Director may appear as an intervener, to independently assist the Tribunal.[362] An agency does not itself initiate proceedings.[363]

6.15 Cases in the Tribunal are by way of rehearing: the Tribunal considers the matter afresh. Neither the Privacy Act, nor the Human Rights Act and Regulations made under it,[364] provide much guidance as to 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, and pleadings. Parties may call evidence and cross-examine witnesses.[365]

6.16 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 a number of remedies including a declaration, a restraining order, an order to perform a specific remedial act, and damages (of up to $200,000).[366]

6.17 The Tribunal hears an average of 17 privacy cases a year. They comprise about half the Tribunal's workload. Declarations and damages are the most commonly awarded remedies. The highest damages award on record is $40,000.[367] A dissatisfied complainant can appeal to the High Court.[368] There may be a further appeal with leave, on a question of law, from a decision of the High Court.[369]

Conclusions about the current process

6.18 The complaints process is modelled in part on the Ombudsmen and Human Rights Acts. Parliamentary debates on the Privacy Bill indicate that the complaints process was intended to provide speedy, low-cost, informal and non-adversarial resolution of complaints wherever possible. The priority was 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.[370] The process is effective in settling the vast majority of complaints.

361 Privacy Act 1993, s 83.

362 Privacy Act 1993, s 86.

363 Evans, above n 353.

364 Human Rights Review Tribunal Regulations 2002.

365 Ibid, reg 19.

366 Privacy Act 1993, s 85. The monetary limit on damages is imposed by the Human Rights Act 1993, s 92Q, which in turn refers to monetary limits in the District Courts Act 1947, ss 29–34.

367 *Hamilton v The Deanery 2000 Ltd* [2003] NZHRRT 28.

368 Human Rights Act 1993, s 123.

369 Human Rights Act 1993, s 124.

370 (20 April 1993) 534 NZPD 14729.

6.19 However, our research and consultation have persuaded us that the policy parameters need re-examination. We think two broad areas need attention. The first is that the present system does not always provide a solution as quickly or efficiently as it should. There are elements of the current process that are cumbersome, confusing, and less than optimally efficient. The second is that a system based solely on *complaints* is not always adequate to resolve problems. A complaints process is necessarily ad hoc and piecemeal. It may succeed in resolving individual cases, but is not so good at detecting and solving systemic problems.

6.20 To address these problems we developed some proposals for reform which we put out for consultation in our issues paper. The proposals were developed in consultation with the Privacy Commissioner.

6.21 We listed the aims of possible reform in our issues paper. We repeat that list here. The reforms 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 easier from the alternative dispute resolution methods at the beginning of the process to the formal determination stage later;
- 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 provide some 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 his or her investigative resources in areas of broader public interest and importance; and
- meet international expectations (information flows and privacy protection now being matters of international concern).

6.22 We made it clear that the proposals were simply that: they were put forward for comment and reaction. We received some very helpful submissions which have assisted us to frame our final recommendations. We now go through the proposals in the issues paper, and state the conclusions we have reached. We deal with them under the two broad headings we indicated in paragraph 6.19.

The harm threshold

6.23 The first proposal was to remove the requirement in section 66 that there must be harm, actual or potential of a kind specified in the section, before a complaint can proceed. Rather, the degree of harm suffered should be a factor in the exercise of discretions such as whether to continue an investigation or refer a complaint to the Tribunal, and in the Tribunal's determination as to what remedy to award.

6.24 We were told that the harm threshold works imperfectly in filtering out less deserving cases. Removing the harm requirement would be easier for complainants to understand, would allow more consistent enforcement, and, in particular, could be useful in exposing systemic problems which have the potential to cause harm if left unattended to.

6.25 The threshold for harm in the Act is that the action complained about has resulted in or may result in harm.[371] In other words, the test is the possibility rather than the likelihood of harm. Yet, although this threshold is quite low, the Tribunal takes the view that the possibility needs to be clearly demonstrated; it is not simply to be assumed. It can be difficult to demonstrate in relation to some principles: principles 1 to 3, for example.

6.26 A considerable majority of submissions to the issues paper were critical of the proposal to remove the harm threshold, and thought that it should stay. They noted that its removal would be likely to lead to an increase in the number of trivial complaints. While many of these would probably be rejected by the Commissioner under the power conferred by section 71 of the Act, it is nonetheless hard to justify the expenditure of public and agency resources dealing with complaints about alleged conduct which cannot be shown to cause harm to anyone. There were also concerns that the absence of a harm threshold could lead to "gaming" the system by using the complaints process for illegitimate purposes: for example, to delay adverse action in relation to a welfare benefit or ACC payment.

6.27 To some extent the "harm" threshold involves a question of perception. Agencies may feel less accepting of the Privacy Act if their freedom of action is open to complaint even though they have done nothing to hurt anyone.

6.28 Two knowledgeable commentators said:

> Such a change would be significant. It would swing the pendulum a long way from the fundamentally remedial nature of Tribunal proceedings towards a far more regulatory model.
>
> I disagree that the harm threshold should be removed. This is a valuable sifting mechanism. It lies at the heart of New Zealand's harm-based approach. To make inroads into that would be to go against one of the great strengths of our legislation.

371 Privacy Act 1993, s 66(1)(b).

6.29 We think that on balance these negative arguments are the more persuasive and believe that the present harm threshold for complaints should be maintained. We note again that it does not require proof that harm has actually occurred, merely that it may occur.

RECOMMENDATION

R54 The harm threshold in section 66 should remain in relation to complaints.

The role of the Director of Human Rights Proceedings

6.30 At present, the Act separates conciliation and litigation functions, so that the Commissioner's ability to conciliate is not affected by also having an enforcement role. The current complaints system changes substantially at the point at which a meritorious complaint which has been unable to be settled is referred by the Privacy Commissioner to the Director. The Privacy Commissioner has said:[372]

> One might see it as marking the change from ADR [alternative dispute resolution] to enforcement. In the ADR phase, the Privacy Commissioner is the "honest broker" that seeks to understand the matter at dispute and to bring the parties to a settlement or render an independent and expert opinion on whether the law has been broken. By contrast, the Director is often informally referred to as an "independent prosecutor". The Act establishes a clear separation so that the somewhat neutral role that the Commissioner performs is not undermined by the enforcement-orientated role.

While we can see the point of the "split" model, it does raise some questions.

6.31 First, while it is sometimes believed that the "split" model makes it easier for OPC to achieve settlements because it is not an "enforcer", it is far from clear that that is in fact the case. It is not immediately apparent why someone should be less ready to settle because the intermediary has functions other than negotiation and persuasion. The idea of a single regulator with a mix of powers is by no means unknown.[373]

6.32 Secondly, there seems to be some ambiguity as to how the Director is perceived: whether he or she takes cases to the Tribunal for the Privacy Commissioner, or whether the Director is independent in all respects and takes a fresh look at all cases. The Privacy Commissioner has commented that "The split is not well understood by participants who are new to the system."[374]

6.33 Thirdly, the present system seems duplicative and inefficient. The Director gets limited information from the Privacy Commissioner, and has to investigate the matter himself or herself. The parties may well think that all the processes they have been through with the Privacy Commissioner have to be repeated with the Director, and that it all takes too long. The Director's involvement may be seen as just another step in a long, convoluted and "clunky" process. It is complex, and may well be confusing for the parties.

372 Office of the Privacy Commissioner *Enforcement, Compliance, Complaints: A Proposal to Reform the Privacy Act* (2009) at [3.32]–[3.33] [*Enforcement, Compliance, Complaints*].

373 See for example the Financial Markets Authority Act 2011, s 9.

374 Office of the Privacy Commissioner *Enforcement, Compliance, Complaints*, above n 372, at [3.34].

6.34 There is a real question of whether the benefits of the present system outweigh the disadvantages.

6.35 We therefore proposed in the issues paper that the Director should no longer be involved in privacy cases.[375] Rather, the Director's "litigation" role would be taken over by OPC. That is, the Commissioner would himself or herself decide whether the case should proceed to the Tribunal, and would act as the plaintiff in the Tribunal. (This would of course not affect the right of the individual concerned to take his or her own proceedings if the Privacy Commissioner does not do so.) The difference between the proposed new process and the current process can be seen by comparing Figures 1 and 2 at the end of this chapter. The current power of the Director in section 20 to institute proceedings for a declaratory judgment would also vest in the Commissioner.

6.36 There are possible disadvantages in such a development. The new responsibilities would require resources to deepen OPC's litigation capability. There could also be something of a change in the perception of OPC. Its transition from a conciliator to an enforcer might possibly make some settlements harder to achieve, although that is speculative: it is equally likely that in some cases it might have exactly the opposite effect.

6.37 The majority of the submitters to our issues paper agreed with the proposal that the Director should no longer be involved in privacy cases. The minority who disagreed did so mainly for the reason that OPC's neutrality might be compromised. We heard the view that a "Chinese wall" might have to be created, and that there thus would still need to be a two-stage process, even though both steps would be carried out in the same office.

6.38 However, we think that these potential disadvantages are outweighed by the speedier and more efficient arrangement which would result. It would benefit the agencies and members of the public involved, and be better understood by them. Legal processes should be as simple, speedy and efficient as possible. It might also be thought that OPC would benefit from being perceived as having some "teeth" rather than as simply a "persuader" with little ultimate authority.

6.39 The complexity of the present system does not increase public confidence in it. The proposed system would be better understood by the parties, and should be more cost-effective. Any concerns about neutrality being compromised could be mitigated by the appointment of a Deputy or Assistant Commissioner in OPC with sole responsibility for taking cases to the Tribunal. We would note that our recommendation extends to the Director only in his or her privacy jurisdiction, not in the Director's other roles.

RECOMMENDATION

R55 The role of the Director of Human Rights Proceedings should be removed in privacy cases. The Privacy Commissioner should decide which cases are to proceed to the Human Rights Review Tribunal and act as the plaintiff in those cases, and perform the other roles currently performed by the Director.

375 Issues Paper at [8.50].

Access reviews

6.40 In the issues paper we proposed that complaints under principle 6, the access principle, should be determined by the Commissioner.[376] We shall call these "access reviews". Currently the Commissioner determines no complaints at all, but instead attempts to reach a settlement. The only body which can make decisions is the Tribunal.

6.41 Our proposal would leave all other complaints as they are, but enable access reviews to be determined by the Commissioner. This would extend not only to straight refusals of access, but also to cases where access is granted on unreasonable conditions (such as an excessive charge).

6.42 There are several reasons why we said 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. Furthermore, although the statute uses the generic term "complaint", complaints involving refusal to give access to information are really reviews of the agency's grounds for refusal. OPC 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. 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.

6.43 A substantial majority of submitters favoured this proposal. Former Privacy Commissioner Sir Bruce Slane noted that the current procedures for dealing with these reviews are "time-consuming and expensive".

6.44 The submitters who disagreed again made the point that it would lead to a confusion of roles in OPC (conciliator on the one hand, decision-maker on the other), and expressed a distrust of the "Chinese wall" that may be necessary. One submitter said that access cases can, more than others, give rise to differences of interpretation between the Privacy Commissioner and agencies, and that it would therefore be better to continue with the present arrangement whereby any actual decision is made by the independent Tribunal.

6.45 We have not been persuaded to differ from our original proposal. The quick and efficient resolution of access cases will be beneficial, especially in cases where the information sought is important to the individual, and is needed quickly. As we said previously, regulators can have a multiplicity of functions, and we think it highly unlikely that a power in the Commissioner to resolve some issues will lead to fewer settlements in the other kinds of case. The concern about differences of interpretation to which we refer in the previous paragraph can be met by a robust right of appeal.

6.46 The Ombudsmen opposed the proposal on the basis that it would lead to a different process between access requests by an individual under the Privacy Act, and access requests by a body corporate under the Official Information Act

376 Ibid, at [8.45]–[8.49].

1982 (OIA). (Bodies corporate cannot make access requests under the Privacy Act: section 34 of that Act provides that only "individuals" can so apply. Bodies corporate can only make access requests to public bodies under the OIA;[377] if they are refused access under that Act they can complain to the Ombudsmen, whose power is confined to recommendation.) We agree that this may sound anomalous, but note that the processes under the two Acts are not the same now; for example, bodies corporate have no recourse to the Tribunal. We also note that in our issues paper on the Review of Official Information we suggest a strengthening of the Ombudsmen's powers in access cases.[378]

6.47 We therefore recommend that the Act should be amended to give the Privacy Commissioner power to determine complaints about access to personal information. We would hope that in many cases the agency complained against will voluntarily agree to release the information anyway, without the need for such determination.

6.48 We propose that if the Commissioner's determination were in favour of the requester, that determination would be accompanied by a notice to release the information. If there was non-compliance with that notice, it could be enforced, at the instigation of the individual, by an order of the Tribunal. The Tribunal has sufficient sanctions at its command to enforce compliance.

6.49 A determination would be appealable to the Tribunal by either party, requester or agency. We think it should be an appeal on the merits.

6.50 There is, however, a further question. We would not envisage giving the Privacy Commissioner power to make an award of damages in relation to a refusal of access. The Human Rights Review Tribunal alone should retain the power to award damages. If the complainant wants such a remedy, he or she could file a separate claim, which would proceed to the Tribunal to be heard after the Privacy Commissioner's determination. Any such claim could be heard along with any appeal against the determination.

6.51 We do not suggest that this new process should extend to complaints under principle 7, the correction principle. Such complaints raise different considerations. 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.[379] The question, therefore, is whether, if the Commissioner could "decide" a principle 7 complaint, he or she would need power to order that the material actually be corrected. We thus confine our proposal to access complaints under principle 6.

377 Official Information Act 1982, s 24.

378 Law Commission *The Public's Right to Know: A Review of the Official Information Act 1982 and Parts 1 to 6 of the Local Government Official Information and Meetings Act 1987* (NZLC IP18, 2010) at [11.76].

379 Privacy Act 1993, s 6, principle 7(3).

RECOMMENDATION

R56 The Privacy Commissioner should be able to finally determine access complaints under principle 6 and issue a notice to release the information.

RECOMMENDATION

R57 Compliance with a notice to release information (as referred to in R56) should be able to be enforced by order of the Human Rights Review Tribunal.

RECOMMENDATION

R58 A determination under principle 6 should be appealable to the Tribunal.

RECOMMENDATION

R59 If a complainant seeks damages for failing to obtain access to information, he or she should file a separate claim which would be heard by the Tribunal after a determination by the Privacy Commissioner.

Representative complaints

6.52 In what follows we mean by "representative complaint" a complaint brought by a representative person or body on behalf of a group, all of whose members would be able to make a complaint individually if they chose.[380] The concept is similar to the class action.

6.53 The Privacy Act currently does not prohibit representative complaints; indeed, arguably it contemplates them. Section 67(1) provides:

> *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 [emphasis added].

6.54 There is no requirement that the complainant and the person whose privacy has been interfered with be the same person, although the Commissioner does have a discretion to take no action if the complainant lacks a sufficient personal interest in the subject matter of the complaint.[381] The provisions about action in the Tribunal specifically refer to class actions, although the right to bring such proceedings is confined to the Director:[382]

> The Director of Human Rights Proceedings may, under subsection (2), 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, where the

380 Peter Spiller *Butterworths New Zealand Law Dictionary* (6th ed, Wellington, LexisNexis, 2005) at 262 defines "representative proceeding" as follows: "Where numerous parties to a Court proceeding who have the same interest in the proceedings are represented by one of the parties."

381 Privacy Act 1993, s 71(1)(e).

382 Privacy Act 1993, s 82(4).

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.

6.55 In the issues paper we set out the advantages of representative actions.[383] In summary they are:

- An individual claimant may, in having to present the facts of the complaint personally, suffer an increased sense of invasion of privacy.
- Representative actions can better address systemic failures. A breach affecting a large number of people can be vicariously addressed by the representative action in cases where no one individual might wish to complain.
- Representative complaints may provide a further deterrent by virtue of their higher profile.
- There is a practical benefit of spreading any costs (particularly of legal representation) across a large group of people.

6.56 However, the current provisions are seldom used, and the potential of the representative action has not been realised. One reason may simply be that the Act is silent on the specific mechanisms and processes for representative actions. We think the Act should make clearer and more specific provision.

6.57 Almost all the submissions we received supported this. The answers to our questions about the detail of representative complaints have led us to the following conclusions:

- The Act should specifically provide that representative complaints are permitted.
- While some definitions of "representative proceeding" assume that the representative should be one of the affected group, we prefer that in the present context the representative should not need to be personally affected. This would allow persons and agencies like Consumer NZ or the Children's Commissioner to lay complaints. We believe that section 71 of the Privacy Act gives the Privacy Commissioner sufficient grounds to decline to investigate a complaint if the purported "representative" is an officious bystander with no real interest.
- Complaints to the Privacy Commissioner should be on an opt-out basis. At the complaint stage the matter is not adversarial, and there is no obvious detriment in being included. But those who, for whatever reason, do not wish to be involved should not be required to be. To enable opting out, there should be power in the Privacy Commissioner to publicly notify such complaints.
- If the matter proceeds to the Tribunal, as it is likely to do if monetary compensation is an issue, or if injunctive relief is required, the matter becomes adversarial. In this instance we agree with the submission of the then Chair of the Tribunal that it is better not to have a single requirement of opt-in or opt-out, but rather to allow the Chair in each case to determine who should be notified, and whose consent should be required.

383 Issues Paper at [8.82]–[8.84].

RECOMMENDATION

R60 The Privacy Act should specifically provide that representative complaints are permitted, and provide more detail about them. It should provide that:

- the representative need not be personally affected;
- complaints to the Privacy Commissioner should be on an opt-out basis; and
- if the matter proceeds to the Tribunal, the Chairperson should determine who should be notified and whose consent should be required.

Human Rights Review Tribunal

6.58 In this section we shall make three points about the Tribunal. First, we have argued elsewhere[384] that such are the responsibilities of the Tribunal, and such the constitutional importance of some of the cases before it, that its Chairperson should be a District Court Judge. The Tribunal can award damages at the same level as the District Court (a maximum of $200,000). It can commit for contempt. It can declare legislation incompatible with the New Zealand Bill of Rights Act 1990. Some of its cases have a political dimension that makes judicial independence very desirable. Currently the Chair is appointed for a fixed term without tenure, and his or her salary is fixed at a daily rate. That is thoroughly unsatisfactory. All submitters who answered this question agreed: indeed, one would even prefer High Court Judge status.

6.59 Secondly, we also received comment that the Tribunal's rules of procedure need revision to remove uncertainties which currently exist. We agree that that would be a useful exercise.

6.60 Thirdly, another question we have been invited to consider relates to the remedies able to be awarded by the Tribunal. In particular, there is a question of whether it should be able to award exemplary or punitive damages where a breach is intentional or in flagrant disregard of the plaintiff's rights. Currently the Privacy Act appears not to allow that: section 88 provides that damages may only be awarded in respect of three kinds of damage.

6.61 There has long been controversy about the concept of exemplary damages in the common law. A judge of the New Zealand Supreme Court has recently described them as "anomalous".[385] In *Mosley v NGN*,[386] Eady J ruled in the English High Court that they were not available in a common law privacy claim. While it may well be that a New Zealand court would not follow Eady J in such a case, we are not inclined to extend the Human Rights Review Tribunal's remedial jurisdiction in this way. Anomalies should not be legislated for without good reason. The Privacy Act is explicit that damages may be recovered for humiliation, loss of dignity and injury to feelings. A flagrant or particularly serious breach of privacy is likely to result in such injury, and an award of

384 Ibid, at [8.56]; Law Commission *Tribunal Reform* (NZLC SP20, 2008) at [7.23]–[7.24].

385 *Couch v Attorney-General* (No 2) [2010] 3 NZLR 149 at [178] per Tipping J.

386 *Mosley v NGN* [2008] EWHC 1777 (QB).

compensatory damages should normally be able to reflect such aggravated hurt to feelings without the inclusion of a distinct punitive element.[387] The Tribunal can award damages of up to $200,000.[388]

RECOMMENDATION

R61 The Chairperson of the Human Rights Review Tribunal should be a judge at the level of a District Court Judge.

RECOMMENDATION

R62 The Human Rights Review Tribunal should not be empowered to order exemplary damages.

BEYOND COMPLAINT RESOLUTION

6.62 We have come a long way in the 18 years since the Privacy Act was enacted. The rapid advance of modern technology has meant that large corporations and government agencies store and use vast amounts of information about people. If their systems, practices and security arrangements are not adequate, damage can be done. Information about people (which may include sensitive financial or health-related information) can get into the wrong hands and be used for the wrong purposes; more information than is necessary for the agency's purpose may be collected; unfair collection methods may be used. As we note below[389] in the discussion of a possible audit power, stories of major security lapses from time to time appear in our media.

6.63 In contexts like these, the complaints system can be an inadequate response. The Commissioner may be unable to take any effective action. In a paper written for discussion with us, the Privacy Commissioner summarised the shortcomings of the complaints system as follows:[390]

> First there is the issue common to any system relying only on complaints: a breach has already occurred when a complaint is made. A Privacy Act compliance system needs to be effective wherever serious risks are identified and not simply rely upon "after the event" redress.
>
> Second, there is the fact that complainants typically see only a small outward manifestation of information systems. The greater part is invisible to them. Relying upon complaints and complainants will be an ineffective strategy for larger systemic issues. The Act needs to affect the decision-making and activities of those "back office" people who design and operate the systems, to promote or require compliant behaviour, and provide tools to the regulator to know or find out more than potential complainants can by themselves.

387 See the discussion of aggravated damages in *Siemer v Stiassny* [2011] NZCA 106 at [50]–[56] per Hammond J.

388 Human Rights Act 1993, s 92Q(2).

389 Below at [6.97]–[6.99].

390 Office of the Privacy Commissioner *Enforcement, Compliance, Complaints*, above n 372, at [3.6]–[3.9].

> Third there are aspects of the design of the current statutory complaints machinery which limit the potential effectiveness of complaints in several contexts including:
>
> - cases where non-compliance is suspected but complaints are not received;
> - a breach of a principle is identified but no "harm or detriment" element is yet manifest;
> - complaints are settled but agency practice does not change.
>
> Finally, the following dynamics of the current system are not conducive to strongly encouraging voluntary compliance:
>
> - agency liability is limited to the harm to the complainant, [and] it may be cheaper to settle a series of complaints than to change a non-compliant system;
> - complaints are handled in private and thus non-compliance resulting in a complaint typically does not involve a risk to agency reputation.

6.64 We asked OPC to provide us with some examples of cases where the complaints system had proved less than adequate. It did so. The examples included the following:

- A professional firm persisted in refusing clients access to information despite multiple OPC case notes, a Tribunal decision and explicit guidance from the professional body.
- Dominant players in an industry failed to meet requirements of a tailored industry code of practice. One upheld complaint resulted in offending data being removed from the single complainant's file, while leaving the same data appearing on thousands of other files.
- Sensitive information continued to appear on a website during protracted negotiations for the settlement of a complaint.
- A public report on an inquiry into an industry practice which was highly critical of that practice failed to influence the behaviour of the companies concerned.
- There was misleading cold calling of consumers seeking financial details, but it was difficult to prove that a particular complainant had suffered the damage necessary to uphold the complaint (as will often be the case with breaches of principles 1–3).

6.65 In a modern age, we think the Privacy Commissioner needs further powers. The office should not be perceived as a "toothless tiger". There are, we understand, instances of large organisations being unreceptive to persuasion. Members of the public who raise serious privacy issues sometimes express surprise and frustration that the Commissioner is unable to do anything. We quote from an international commentator on privacy law:[391]

> Data Protection Commissioners are a form of highly specialised ombudsmen with a more active part to play than the classic role of responding to individual complaints. It is not enough to respond to repeated similar grievances from a changing cast of individuals. The staff has to pursue general systematic improvements in information handling practices by using a variety of methods.

391 David Flaherty *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989) at 400.

6.66 As one example, the UK Information Commissioner has a large number of tools available. They include criminal prosecution, enforcement notice, monetary penalty notice (for an amount up to £500,000), application for an enforcement order, and compulsory audit. Enforcement tools which can be used in connection with these powers include an information notice, an assessment notice and a search warrant.[392]

6.67 We would not wish to go so far in New Zealand, but think that the Privacy Commissioner's powers should be enhanced in two ways.

Compliance notices

6.68 First, we recommend that the Privacy Commissioner should have power to issue compliance notices: in other words, to issue directions to an agency requiring it to take certain action, or to desist from taking certain action, in order to comply with the requirements of the Act. Subject to some limitations we shall outline shortly, the notice would bind the agency to comply, and failure to do so would result in a penalty.

6.69 A problem requiring a compliance notice might be brought to light by a complaint, but might also come to the Commissioner's attention in a number of other ways: as the result of an audit; by the media; by an inquiry conducted under section 13(1)(m) of the Privacy Act; or by a security lapse or "data breach".[393] The power to issue notices would enable the Commissioner to address the kinds of problems manifested in the examples the Commissioner provided to us. It would enable cases of the following kinds to be addressed:

- Breaches have been identified, but there has been no complaint, perhaps because individuals are deterred from complaining for fear of adverse consequences.
- There has been repeated non-compliance despite requests to desist or change practices.
- Even after settlement of a complaint, agency practice does not change and there remain deficiencies in its systems which need to be corrected for the future.
- There have been systemic breaches where no harm has yet occurred, but which can be proactively rectified before there is harm.
- Assurances have been given in the course of settling a complaint, but have not been given effect to. (Currently the Act anticipates that assurances may form part of a settlement, but does not provide for any sort of enforcement if an assurance is breached.)
- A complaint relates to only one part of a larger systemic issue.

392 Information Commissioner's Office (UK) "Data Protection Regulatory Action Policy" (10 March 2011) at 2–4.

393 See ch 7.

6.70 Such a system would give the Commissioner a discretion to differentiate between, on the one hand, the majority of agencies that try to comply but fall short on occasions; and, on the other, a small proportion that make insufficient effort to comply, or even deliberately engage in non-compliant behaviour if it offers advantages to them. A differentiated response according to the conduct in question makes the system more meaningful to everyone.

6.71 Moreover, a compliance notice system could save time and resources. A direction to put a systems failure right might remove the need to engage in days of repeated persuasion; it might also avoid the need to investigate a string of separate complaints. It may be a short and sharp solution, but it can be an efficient one.

6.72 A considerable number of Privacy Commissioners in cognate jurisdictions have such powers, although they are called by a variety of names, including "orders", "notices" and "determinations". Such powers are found, for example, in British Columbia and Ontario, the United Kingdom, Victoria, Queensland and Australia (Commonwealth). A survey carried out in 2010 by the International Association of Privacy Professionals recorded that 26 out of 38 respondent data protection authorities had the power to issue cease-and-desist orders.[394]

6.73 The concept of the compliance notice (or demand notice or enforcement notice) is well known in New Zealand in other contexts, and appears in a number of statutes. They include our employment legislation,[395] finance and market legislation,[396] health legislation,[397] the Resource Management Act 1991,[398] the Education Act 1989,[399] the Public Transport Management Act 2008,[400] and the Hazardous Substances and New Organisms Act 1996.[401] Even though the contexts of some of these Acts no doubt differ from the Privacy Act, they demonstrate that there is nothing constitutionally unusual about such a power in a regulator. Closer to the subject matter is the Public Records Act 2005, which concerns information handling just as the Privacy Act does: under that Act the Chief Archivist has specific powers to direct government agencies on certain matters.[402] Even the Privacy Commissioner already has such a power, although it is confined to one situation: as a result of an amendment to the Privacy Act in 2010, the Commissioner can issue notices prohibiting the transfer of information overseas.[403] It would be a strange irony if the Commissioner had such a power to protect overseas persons yet not to protect New Zealand citizens.

394 International Association of Privacy Professionals "Data Protection Authorities: 2010 Global Benchmarking Survey: Executive Summary and Findings" (2010) at 12.

395 Employment Relations Act 2000, s 224; Holidays Act 2003, s 77; Volunteers Employment Protection Act 1973, s 14ZQ.

396 Securities Marketing Act 1988, ss 34, 36YD, 36ZO; Takeovers Act 1993, s 32; Insurance (Prudential Supervision) Act 2010, s 106; Commerce Act 1986, ss 53ZD, 74A; Financial Advisers Act 2008, ss 49, 73.

397 Health and Safety in Employment Act 1992, s 39; Health Act 1956, s 69ZZH.

398 Resource Management Act 1991, ss 322, 329.

399 Education Act 1989, ss 35J, 255A.

400 Public Transport Management Act 2008, s 44.

401 Hazardous Substances and New Organisms Act 1996, s 66.

402 Public Records Act 2005, ss 31, 37, 39.

403 Privacy Act 1993, s 114D.

6.74 A majority of the submitters to our issues paper supported a power to issue compliance notices. However, a significant minority did not. This minority comprised some large agencies in both the public and private sectors. Their main arguments are as follows.

6.75 First, some believed that the power to issue compliance notices would change the culture of OPC, and the way it is perceived by agencies. It would become an "enforcer" rather than a "persuader". Yet there is nothing inconsistent about a regulatory agency having a mixture of persuasion, negotiation and enforcement powers. In such an "enforcement pyramid" model,[404] the compliance order stands at the top of the pyramid to be utilised only when the other modes of resolution have failed. It would be a "last resort" power. We do not think that it would make OPC a different kind of office, although it might to some extent change the way it is perceived.

6.76 Secondly, as we have noted above, a compliance notice could be triggered in a number of ways, among them an audit. But it could also be triggered by a complaint. There is, no doubt, a distinction between the resolution of a complaint between the parties and the issuing of a compliance notice to correct an underlying problem. The recompense provided to the individual complainant for any harm suffered would be separate and apart from the notice to cease or change the practice in question. It may even be that the matter that is the subject of the notice might not have been the subject of the complaint, but may have been discovered in the course of investigating it. But that distinction may be too subtle for some, who will see a compliance notice as a possible outcome of a complaint. This might change the perception of the complaints process. It may lead to a less cooperative and more adversarial attitude from the start, particularly when the agency complained against is represented by a lawyer. Sir Bruce Slane supported such a power, but he was concerned about precisely this point. He said:

> It should be acknowledged that when the Commissioner does more than give an opinion, there may be less co-operation with the investigative process. Knowing that the outcome was not binding did, in my opinion, lead to co-operation and there were fewer lawyer-driven blocking attempts than might otherwise have been mounted.

6.77 However, while there may be a more adversarial attitude in some cases, we think it is just as likely that in others the existence of such a reserve power may lead agencies to be more willing to reach a settlement. Furthermore, in the great majority of complaints the possibility of a compliance notice will simply not be an issue: they will proceed to settlement exactly as they do now.

404 For a discussion of the "enforcement pyramid" concept, see Ministry of Consumer Affairs *Review of the Redress and Enforcement Provisions of Consumer Protection Law* (2005) Part 2; Australian Treasury *Review of Sanctions in Corporate Law* (2007) at [1.21]–[1.32].

6.78 Thirdly, a number of submitters questioned the need for such a power, saying that there is presently no evidence of systemic failure which would justify the existence of compliance notices. We are satisfied that this is not the case. We have already referred to some of the examples given to us by the Privacy Commissioner.[405]

6.79 Fourthly, the Privacy Commissioner is one of a group of regulatory authorities which operate a complaints system without power to issue enforcement notices. The others include the Human Rights Commission, the Health and Disability Commissioner, and the Ombudsmen. So the Privacy Act is part of a wider model relying on mediation, persuasion and settlement. It may be asked, if these other agencies have no directive power, why should the Privacy Commissioner have such a power? Why is privacy different from the other rights-type issues with which these other offices deal?

6.80 In relation to the Ombudsmen it is not quite right to say that they have no directive power: in relation to Official Information Act, an Ombudsman's recommendation to release information creates a duty to comply (albeit one which can be "vetoed" by the Governor-General in Council).[406] In relation to the Ombudsmen's other functions, they exist only in relation to government agencies, and non-compliance can be sanctioned by an Ombudsman reporting the matter to the Prime Minister, and making a report to Parliament. These are strong sanctions.

6.81 As to the Human Rights Commission and the Health and Disability Commissioner, one answer may be that the Privacy Commissioner has to deal more often with large organisations where non-compliance can prejudice thousands of people. But another may simply be that those other Commissions would also benefit from such powers.

6.82 Fifthly, it may be argued that since the Tribunal already has power to make what are effectively compliance orders, a restraining order under section 85(1)(b) and an order to remedy an interference under section 85(1)(d), there is no need for a power in the Privacy Commissioner. But these orders, while valuable and potentially far-reaching, are usually dependent on a complaint. More importantly, cases can sometimes take a long time to be heard by the Tribunal; sometimes urgent action is necessary to stop an abuse. A compliance notice process is more straightforward and less expensive.

6.83 We have considered this matter with care, and have reached the clear conclusion that the Privacy Commissioner should have the power to issue compliance notices. We so recommend. We envisage that such notices will be infrequent and will be a fall-back measure when a request to comply has failed.

405 Above at [6.64].

406 Official Information Act 1982, s 92.

Implementation

6.84 The details of a new compliance notice system will need to be spelled out in the legislation:

- The Privacy Commissioner should have power to issue such notices in respect of any breach of the Act, whether of the privacy principles or of a substantive provision of the Act (such as the obligation to appoint a privacy officer in section 23 and the obligation to take precautions to correctly identify requesters in section 45).
- Matters to be taken into account before exercising the power should be specified, although the list need not be exhaustive. They should include such matters as the other measures which have been taken, or might be taken, to obtain compliance; whether the agency has taken a cooperative approach; the likelihood of recurrence; the number of people who might be affected by the breach; and the extent of the non-compliance. The occurrence of harm should not be a prerequisite, for sometimes the advantage of a notice can be that it will prevent the occurrence of harm.
- Notices should be able to be issued in relation to matters discovered as the result of a complaint or in any other way.
- The agency should have the right to be heard before a notice is issued, whether by written or oral submission.
- There should be a right of appeal to the Tribunal against the issuing of a notice.
- The Commissioner should have a discretion to publish the fact that a notice has been issued.

6.85 The next question is what sanctions there should be for non-compliance with a notice.

6.86 There are three options. The first is to provide that the notice immediately imposes an obligation to comply, and that non-compliance is an offence punishable by a fine. That would be equivalent to the power to issue an injunction with immediately binding effect. If the respondent wished to appeal the notice, it would have to request at the same time a stay of the otherwise immediate effect of the notice. The second is to provide that in the case of non-compliance with a notice, the Privacy Commissioner could apply to the Tribunal for an enforcement order. Non-compliance with the order would then constitute an offence. This is the model used, for example, in the Public Transport Management Act 2008.[407] But it seems cumbersome in this context, and would effectively mean that the notice was little more than a warning. In urgent matters it would be unsatisfactory. The third option takes a middle way between the other two. It is the solution we put forward in the issues paper, and we continue to support it. The compliance notice would specify a time within which it could be challenged in the Tribunal. If not challenged within that time, it would become enforceable. If challenged, the matter would be considered by the Tribunal; the notice would either be disallowed, or issued as a Tribunal order. There are analogies with abatement notices under the Resource Management

407 Public Transport Management Act 2008, ss 44, 45.

Act 1991[408] and demand notices under the Employment Relations Act 2000.[409] There is a precedent in the Victorian privacy legislation.[410] Once the notice became enforceable or was embodied in a Tribunal order, non-compliance would be an offence punishable by a fine. We recommend this option. The legislation should set the fine at an appropriate level. That prescribed in the 2010 amendment in relation to transfer prohibition notices is $10,000, whereas the standard fine for other Privacy Act offences (set in 1993) is $2,000.

6.87 We think it would also be most helpful if the Privacy Commissioner published a protocol for how the power will be used. We would expect that protocol to emphasise that the compliance notice is a last-resort power, and that it is not expected that it will be frequently used.

RECOMMENDATION

R63 The Privacy Commissioner should have power to issue compliance notices. The Act should provide as follows:

- The power should lie in relation to breaches of the information privacy principles or any other statutory duty imposed by the Act.
- The matters to be taken into account before making an order should include:
  - other possible means of securing compliance;
  - whether the agency has been cooperative;
  - the likelihood of recurrence;
  - the number of people who might be affected by the breach; and
  - the extent of the non-compliance.
- Notices should be able to be issued in relation to matters discovered as the result of a complaint or in any other way.
- The agency should have the right to be heard before the issue of a notice.
- There should be a right to challenge the notice in the Human Rights Review Tribunal.
- If the right of challenge is not exercised the notice should become enforceable; if the right of challenge is exercised and does not succeed, the Tribunal should issue an enforcement order.
- The Commissioner should have a discretion to publish the fact that a notice has been issued.
- Non-compliance with an enforceable notice should be an offence under the Privacy Act.

408 Resource Management Act 1991, ss 322, 325.

409 Employment Relations Act 2000, ss 224, 225.

410 See Information Privacy Act 2000 (Vic), ss 44, 48.

A power of audit

6.88 Currently, by virtue of section 13(1)(b) of the Privacy Act, the Commissioner can conduct a privacy audit of an agency if the agency requests it. This provision, which has been in the Act from the beginning, is some recognition that audits have value in promoting compliance. However, there have been no requests in the life of the Act to date, and therefore no audits. The question is whether the Privacy Commissioner should have power to *require* audits.

6.89 In this electronic age, large agencies deal with masses of information about people. Sometimes that information is shared with others; sometimes its processing is outsourced. If security and information-handling practices are poor, there is a real risk of detriment to the people involved. It is in the interests of everyone, including the agency itself, to have sound systems.

6.90 In our earlier discussion of the complaints-driven system,[411] we noted its shortcomings. It operates after the event rather than being preventative; a complaint may deal only with a small aspect of what may be a wider systemic failure; even though non-compliance may be suspected, no complaint may yet have been received. We noted above some examples of cases where the complaints system has been inadequate to deal with non-compliance.

6.91 A power of audit would enable the Commissioner to be proactive in promoting compliance with the Act without having to wait for a complaint. The existence of such a power would be an incentive to agencies to comply with the Act. There is nothing like the prospect of an audit to ensure that proper standards are maintained. Moreover, audit is an educative tool: it raises awareness of good practice among agencies and their staff. The United Kingdom Information Commissioner has recently said: "Audit, I believe, has a key role to play in educating and assisting organisations to meet their obligations."[412]

6.92 A system of mandatory audits exists in most analogous jurisdictions, although its application to the private sector is not universal.[413] In Canada, the Privacy Commissioner has power to conduct audits of both public and private sector organisations. The Australian Privacy Commissioner has power to audit public sector organisations. Currently, the Australian Privacy Commissioner can audit a private sector organisation only on request, but the ALRC has recommended that the power of mandatory audit be extended to cover the private sector; the Australian Government in its first-stage response has accepted that recommendation.[414] Until recently, the UK Information Commissioner only had power to conduct audits by consent, but in 2009 was given power to issue an "assessment notice" to a government department or other agency designated by order of the Secretary of State.[415] The United Kingdom Information Commissioner has recently issued a code of practice for these assessment notices, providing the framework for how the ensuing audits will be conducted.

411 See above [6.63].

412 Information Commissioner's Office (UK) *Assessment Notices Code of Practice* (April 2010) at 1.

413 For discussion of the overseas position see Issues Paper at [6.77]–[6.84].

414 *For Your Information* at 1585–1588, R47–6; *Enhancing National Privacy Protection* at 87.

415 Data Protection Act 1998 (UK), ss 41A–41C.

He notes that, while currently his audit powers extend only to government departments, "it is entirely reasonable to expect" that where the evidence supports it he will seek to extend his powers to the private sector.[416]

6.93 In New Zealand, the Privacy Commissioner already has certain powers which might be described as analogous to audit. In the case of information matching, internal audits are used as part of the process of granting authorisation; moreover, every five years a matching programme must be reviewed.[417] It is likely that, if the Law Commission's proposals for information sharing[418] are accepted, there will be a similar review role for the Commissioner. There are also audit provisions in the Credit Reporting Privacy Code: it requires credit reporters to undertake compliance checks.[419] We also draw attention to section 69 of the Privacy Act: it empowers the Commissioner to undertake an "own motion" investigation of "any action that is or appears to be an interference with the privacy of an individual". This power does bear some relationship to audit, although it is an investigation of an *action* rather than of *systems*. It is not often exercised.

6.94 Powers of audit or inspection (other than standard financial audits) are not unknown in other New Zealand legislation. They exist in some health,[420] education[421] and consumer[422] legislation. Some of the powers conferred in these other acts even involve powers of entry and possession of documents, going much further than is necessary in the present context. However, one example which is more closely analogous to the present context is the Chief Archivist's audit duty. Section 33 of the Public Records Act 2005 provides:

> **33 Independent audits of public offices**
>
> (1) As soon as is reasonably practicable after the date that is 5 years from the commencement of this Act, an independent audit of recordkeeping practices must be carried out in every public office.
>
> (2) The Chief Archivist must commission and meet the costs of each audit, which must–
>
> (a) cover the aspects of recordkeeping practices specified for the purpose of the audit by the Chief Archivist; and
>
> (b) be based on criteria developed by the Chief Archivist.

6.95 There is provision for a further cycle of audits at intervals of between 5 and 10 years. It is not easy to see why a privacy audit is inappropriate while a general audit of record keeping is: privacy is about information handling too.

416 Information Commissioner's Office (UK) "Data Protection Regulatory Action Policy" (10 March 2011) at 1.

417 See appendix 2; also Office of the Privacy Commissioner *Information Matching Compliance Auditing Information Pack* (Wellington 2008).

418 See appendix 1.

419 Credit Reporting Privacy Code 2004, rr 5, 8, 11, and sch 3.

420 Health Practitioners Competence Assurance Act 2003, s 124; Health and Disability Services Safety Act 2001, s 32.

421 Education Act 1989, s 325.

422 Motor Vehicle Sales Act 2003, ss 124, 125; Weights and Measures Act 1979, s 28; Food Act 1981, s 8ZV.

6.96 The question, then, is whether in addition to the power to conduct audits on request, the Privacy Commissioner should have power to require audits to be undertaken. We put the question in our issues paper, and it divided submitters. Eight gave unqualified support; eight, while not opposing mandatory audits, expressed some concerns; eight opposed the proposal. Most of the supporters were from the public sector and most of the opponents from the private sector, although that division was not absolute: there were members of the "other" category in both sets of submissions. The arguments against the proposal were clearly stated in the negative submissions.

6.97 First, it was said, audits are unnecessary: there is no evidence of systemic problems and the commercial sector is already incentivised to comply. Yet, from time to time the media carry stories of apparent systems failures which have allowed information to escape into unauthorised hands,[423] or of questionable collection practices.[424]

6.98 In a follow-up to one of these breaches, the *Dominion Post* reported:[425]

> The breach has prompted internet security experts to warn of the "invisible threat" of personal security breaches, with research showing that at least 500 New Zealand websites are susceptible to the most basic security attack.

6.99 In her Annual Report for 2010, the Privacy Commissioner drew attention to "significant health information privacy issues" around certain health records. She also said:[426]

> Our follow-up survey on the use of portable storage devices by government agencies showed generally improved security around their use but some key agencies still need to improve their practices.

6.100 It would, indeed, be remarkable if all agencies had information handling practices which were beyond improvement.

6.101 Secondly, it was said that there could be adverse reputational effects for agencies selected for audit. The knowledge that an agency had been selected for audit, even under a random audit system, could create a stigma. The fewer audits there were, the more this would be so. While this risk cannot be discounted, we do not think it is a serious one. Observers generally do not equate investigation with "guilt", and in any event a privacy audit does not carry the same implications as an investigation for, say, fraud.

423 Susie Nordqvist "Telecom Data Breach Prompts Warning" *New Zealand Herald* (Auckland, 18 January 2011) < www.nzherald.co.nz > ; Amanda Fisher "Security Slips Through the Net" *Dominion Post* (Wellington, 31 July 2010) at A6.

424 Office of the Privacy Commissioner "Google's Collection of WiFi Information" (press release, 14 December 2010); New Zealand Medical Association "Patient Notes – Clarity for Insurers and Doctors" (press release, 29 June 2009).

425 Fisher, above n 423.

426 Office of the Privacy Commissioner *Annual Report*, above n 352, at 10.

6.102 Thirdly, it was again said that the acquisition of an audit role could affect the way in which OPC is perceived: its taking on a quasi-"enforcer" role could prejudice its continuing function as a facilitator. We have at other places in this chapter given our reasons for doubting whether that would be so. Nor is it really correct that audit is an enforcement role: it is at least as much an educational and facilitative one.

6.103 The fourth argument against an audit power is simply that audits can be time-consuming and resource-intensive for both the auditor and auditee. They can direct attention away from core business. That is true, and is a reason for ensuring that the power should be used sparingly, selectively and for good reason. It is not a reason for not conducting audits at all. It is in agencies' interests to manage the personal information that they hold well. The costs of conducting audits must be weighed against the costs of non-compliance with the Act; for example, economic losses for businesses that lose customers' loyalty due to poor privacy practices. There is also a cost in the resources required for the Privacy Commissioner to handle complaints, and this cost could be avoided if audits can reveal non-compliance before a complaint eventuates.

Conclusions on audit

6.104 We think a case is made out for giving the Privacy Commissioner power to require audits. The arguments in favour outweigh those against. The legislation would need to provide for a number of key matters.

6.105 First, who would conduct the audits? That question obviously raises issues of resourcing and capability. We think that it would be best to give the Privacy Commissioner power to decide whether, in a particular case, the audit should be undertaken by OPC; whether another organisation should be commissioned to do so; or whether the agency in question should be required to conduct a self-audit and report to the Commissioner. It might be possible in some instances to combine the audit with another: for example, an audit of a government agency under the Public Records Act.

6.106 Secondly, an audit might be of the whole of an agency's information-handling systems, or of only one or two aspects: for example, its collection practices. One would expect the Privacy Commissioner to be conscious of the resource implications when deciding how extensive an audit should be.

6.107 Thirdly, what would trigger an audit? One could specify no criteria in the Act, but leave it to the Commissioner's discretion to decide whether an audit was appropriate. That has some attractions: it would be less likely to have an adverse effect on an agency's reputation than if the threshold was, say, reasonable grounds for suspecting non-compliance. It would also enable the Privacy Commissioner to be proactive and encourage cross-sectorial compliance. But we are reluctant to confer an unconstrained power to conduct audits at random. It could lead to allegations of waste of resources, especially in cases where it was not immediately apparent to an agency why it had been selected. So, taking into account resource considerations, we prefer a constrained power: a power to conduct audits for good reason. Such reasons could be:

(a) that there are reasonable grounds to believe that an agency's systems are not adequate to protect privacy;

(b) that an agency or agencies are involved in the handling of particularly sensitive information (for example, health information); and

(c) that an agency is engaging in a new and relatively untested practice (such as biometric testing).

No doubt the Privacy Commissioner would also be influenced by considerations of cost. The state of the economy would be a factor in both the number and type of audits.

6.108 Fourthly, there is an issue of whether audits should cover both the public and private sectors. There is a stronger case for auditing in relation to the public sector because it spends public money, and also because competition, which can create an incentive for good practice in the private sector, is lacking in the public sector. Moreover, as noted above, there are already going to be information audits of the public sector under the Public Records Act 2005, and privacy audits are of a kind with those; they could even be conducted jointly with them. As we have seen, in some other jurisdictions audits are confined to the public sector. Nevertheless, both private and public sectors are subject to the Privacy Act, and its range of enforcement measures, as a whole. Moreover, some private-sector bodies deal in sensitive personal information which needs to be particularly carefully guarded. We therefore think the power of audit should apply to both sectors.

6.109 Fifthly, there is a question of what powers would be needed. There would need to be a power to obtain information, so the current powers to require the production of information and to question witnesses would need to be extended beyond the areas to which they are currently confined.[427] Overseas experience indicates that audits are best used as an educative tool rather than a punitive one, so a report on the audit should be given to the agency. However, there should also be a discretion in the Commissioner to make the findings public, to enable others to learn, although in such a case the Commissioner should have a discretion whether or not to publish the agency's name.[428] The Privacy Commissioner will need to write a protocol for audits in which the notice to be given, the process to be followed, and the consequence of audit are clearly stated. The Code of Practice recently issued by the UK Information Commissioner might be a useful precedent. Among the consequences is the possibility of a compliance notice; the protocol should make that clear.

RECOMMENDATION

R64 The Privacy Commissioner should have power to require audits of agencies. This power should have the following features:

- The Privacy Commissioner should have power to undertake such audits personally; to commission another organisation to do so; or to require an agency to conduct a self-audit and report the results to the Commissioner.
- The Privacy Commissioner should have power to require an audit for good reasons. Among the good reasons might be:
  - (a) that there are reasonable grounds to believe that an agency's systems are not adequate to protect privacy;
  - (b) that an agency or agencies are involved in the handling of particularly sensitive information (for example, health information); and
  - (c) that an agency is engaging in a new and relatively untested practice (such as biometric testing).
- The power of mandatory audit should apply to both the public and the private sectors.
- The Privacy Commissioner should have appropriate powers to investigate, question persons and require information.
- The report on an audit should be given to the agency in question, but there should be power in the Privacy Commissioner to publish the findings more widely.

RECOMMENDATION

R65 The Privacy Commissioner should issue a protocol of the processes to be followed for conducting an audit.

427 See Privacy Act 1993, ss 22 and 91.

428 The Commissioner would also have to comply with Privacy Act 1993, s 120, which provides that adverse comment should not be made about a person in a report unless that person has had an opportunity to be heard.

NEW OFFENCES

6.110 The issues paper noted that the Act is enforced primarily through civil remedies rather than the criminal law. We have just recommended, in the discussion of compliance notices, a further role for the existing offence provisions.[429] We now examine the possibility of including two new offence provisions. Both were discussed in the issues paper.[430]

6.111 The first is an offence of intentionally misleading an agency by:

(a) impersonating the individual concerned; or

(b) misrepresenting the existence or nature of authorisation from the individual concerned;

in order to obtain that individual's personal information or to have that personal information used, altered or destroyed.

6.112 This addresses the growing problem of "pretexting". We understand that worrying practices have been exposed overseas, involving systematically misleading agencies to obtain personal information, which may then be traded. Currently, an individual whose personal information has been exposed may be able to complain against the agency for disclosing the information, but there is no sanction against the person who engaged in deception to obtain personal information.

6.113 The second proposed offence is knowingly destroying documents containing personal information to which the individual concerned has sought access in order to evade the access request. This is to deliberately deny people their entitlements. In such a situation the complaints process is ineffective, given that the information no longer exists.

6.114 There was unanimous support for these new offences from 19 submitters, although the Police support was in principle only, and they wish to reserve final judgment until details are settled.

6.115 We recommend these two new offence provisions.

RECOMMENDATION

R66 There should be new offences of:

(a) Intentionally misleading an agency by impersonating an individual or misrepresenting an authorisation from an individual in order to obtain that individual's personal information, or to have that information used, altered or destroyed.

(b) Knowingly destroying documents containing personal information to which a person has sought access.

429 Above at [6.86], R63.

430 Issues Paper at [8.86]–[8.88].

THE OMBUDSMEN'S ROLE

6.116 The issues paper raised a question of whether there should be any change in the Ombudsmen's jurisdiction in relation to OPC.[431]

6.117 A concern was expressed that while Ombudsmen's investigations are normally concerned with process, an investigation could in theory get into substantive matters by holding that an opinion of the Commissioner involved a mistake of law. The fear was that the Ombudsmen might substitute their view for that of the Commissioner. The Ombudsmen's submission made the point that any recommendation they might make is not binding:

> Should the Privacy Commissioner decide not to accept the outcome of an Ombudsmen's investigation then no doubt the Commissioner would have her own good reasons for such a decision. Where there are good reasons for a difference of opinion on matters of fact and law, we are unaware of any case in the history of the Office that an Ombudsmen has formed an opinion on those issues.

There was little support in other submissions for change. All Crown entities are subject to the Ombudsmen's jurisdiction. It is hard to make a case for an OPC exemption when the Human Rights Commission, the Health and Disability Commissioner and the Office of Film and Literature Classification are so subject. We support the status quo.

CONCLUSIONS

6.118 In our view the recommendations in this chapter will, if implemented, improve the present system, and meet the objectives of reform we outlined at paragraph 6.21.

6.119 The removal of the Director of Human Rights Proceedings from the process, and the power in the Privacy Commissioner to make determinations in access cases should simplify the present processes, reduce delay, and make matters easier to understand for agencies and the public alike. The clarification of representative complaints should enable some systemic non-compliance to be dealt with more efficiently than it now is. The proposed power of audit will enable systemic non-compliance to be discovered and corrected. The proposed power in the Privacy Commissioner to issue compliance notices will give the Commissioner more effective power to deal with non-compliant agencies, and will detach effective enforcement from the complaints process. A process which is entirely complaints-driven is of its nature a lottery: some big issues may not result in complaints, whereas smaller, even trivial, matters without general implications may result in too many complaints. A system where persuasion and conciliation are the first step and an enforceable directive a possible end-point gives access to a range of measures appropriate to varying degrees of non-compliance.

6.120 We repeat the conclusion we expressed in our issues paper.[432] 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.

431 Issues Paper at [8.90]–[8.92].

432 Issues Paper at [8.68].

FIGURES: CURRENT AND REFORMED COMPLAINTS PROCESSES

Figures 1 and 2 are simplified depictions of the current and proposed complaints processes. Only those outcomes that result in further steps in the process are shown. Outcomes that involve no further action, such as a settlement being reached or a complainant deciding not to proceed, are not shown.

FIGURE 1: CURRENT COMPLAINTS PROCESS

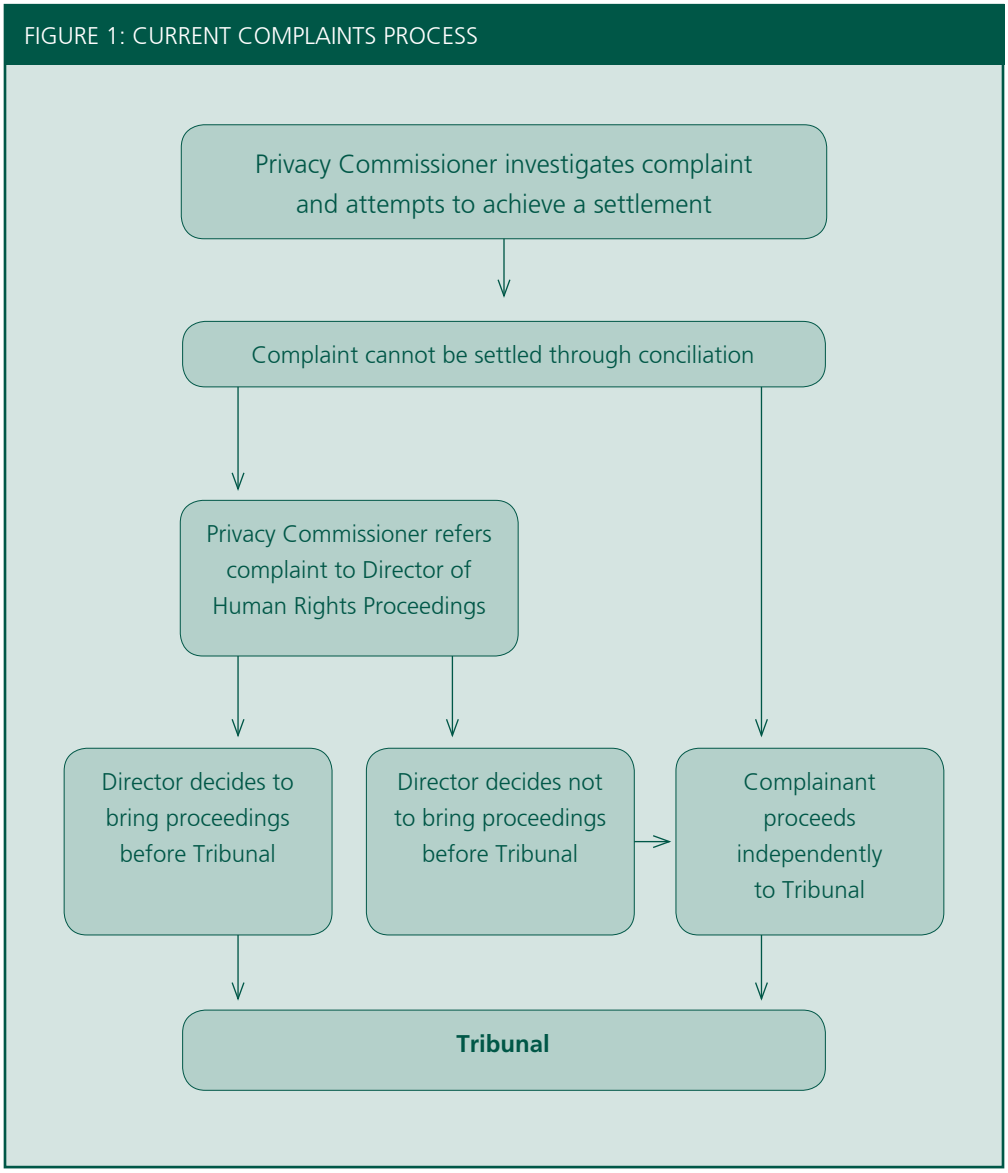
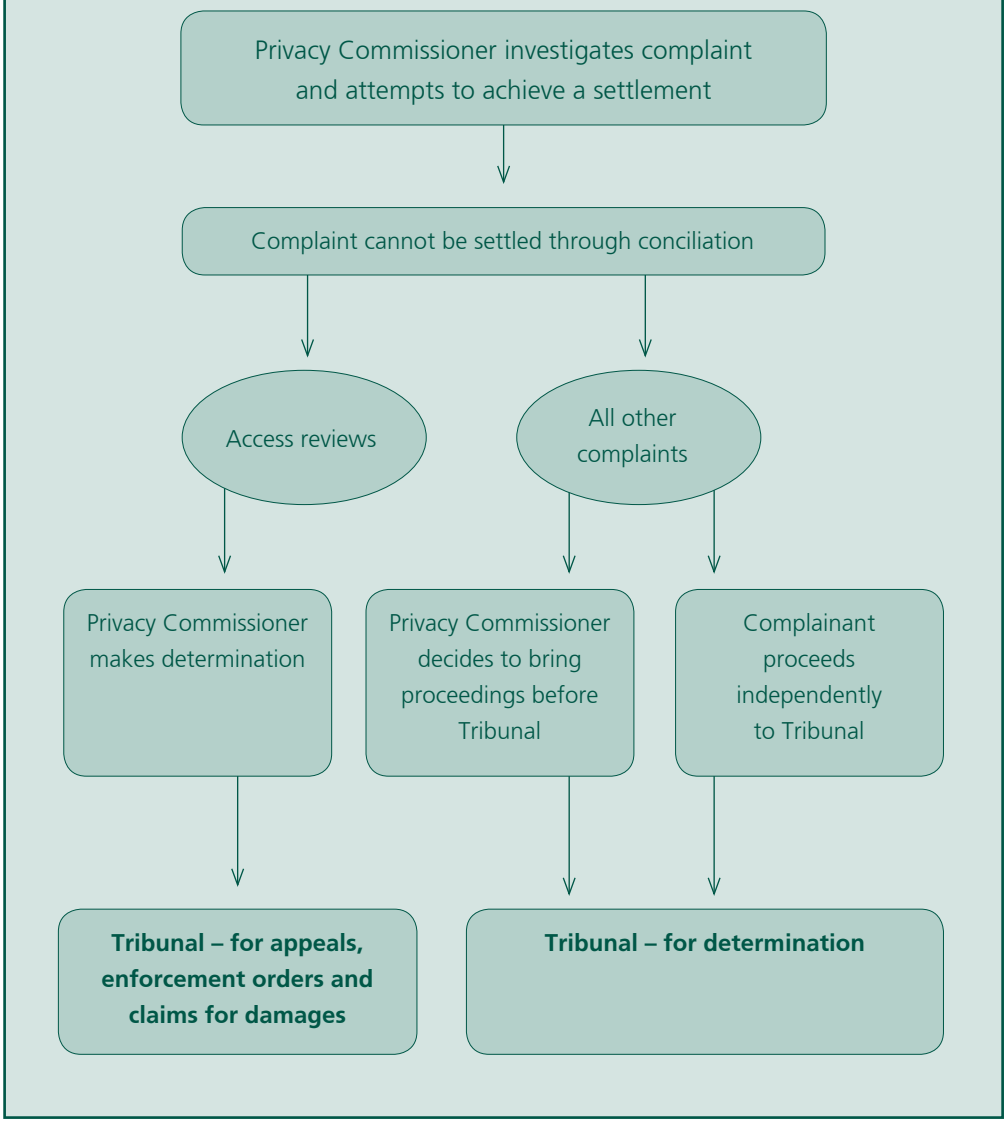


FIGURE 2: REFORMED COMPLAINTS PROCESS



Chapter 7

Data breach notification

7.1 This chapter discusses the merits of introducing into the Privacy Act a mandatory obligation of "data breach notification". "Data breach" is a term in very common use, and we shall use it in this chapter. However, the expressions "data security breach" or "privacy breach" perhaps more accurately describe the concept, and it may be that one of them would be more appropriate when it comes to drafting the legislation. The question simply is: if personal information held by an agency is lost, or accessed improperly, should the agency be obliged to notify the subject of the information? Currently there is no such obligation. The Privacy Commissioner has, however, issued guidelines on good practice in such a situation.[433]

7.2 Given the mass of information that is now being collected and held by organisations, it is inevitable that at certain times personal information will be accessed, discovered or otherwise acquired in a way that is not authorised. Data breaches can take a multitude of forms varying from innocent loss of a file or laptop, or inadequate security, to intentional acts such as computer hacking or "blagging" (obtaining information by deception).[434]

7.3 In New Zealand, recent high-profile data breach examples include the customer databases of a fast-food company and a telecommunications company being accessed illegally, exposing the personal information of large numbers of customers.[435] 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 Customs Service losing two CDs, on which were copies of millions of records containing financial and other details of people in receipt of child benefits (including names, addresses, dates of birth, and national insurance numbers). Another case involved the United Kingdom Ministry of Defence losing a laptop computer

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

434 In relation to blagging, also known as pretexting, see R66(a).

435 For further discussion and examples see Amanda Fisher "Security Slips Through the Net" *Dominion Post* (Wellington, 31 July 2010) at A6; Issues Paper at [16.9]–[16.10].

containing the personal details of up to one million people. Similar large incidents occur in the United States. Stories about such data breaches appear frequently in the media.[436]

DATA BREACH NOTIFICATION IN OTHER JURISDICTIONS

7.4 Mandatory notification laws exist in nearly every state in the United States, and almost 30 of these are based on an original Californian model.[437] Various attempts to enact a Federal breach notification law have, to date, been unsuccessful, although the Obama administration has recently indicated its support for such a law.[438] Financial institutions throughout the United States are subject to mandatory notification obligations under guidelines issued by the Department of the Treasury.[439]

7.5 The European Union has recently amended its e-data Directive covering the telecoms sector (including phone, e-mail, SMS, and internet use) to include a mandatory notification requirement.[440] 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.[441] An all-sector mandatory notification law has also been enacted in Germany,[442] and in Ireland the Data Protection Commissioner has issued a Personal Data Security Breach Code of Practice.[443]

7.6 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".[444] This recommendation was supported by the Australian Office of the Privacy Commissioner.[445] The Australian Government is yet to respond to this aspect of the ALRC's report. However after 1.5 million Australian user accounts were compromised in an attack on Sony's Playstation network in May 2011, the Australian Privacy Minister said that a notification system now "appears necessary".[446]

436 Issues Paper at [16.11].

437 National Conference of State Legislatures "State Security Breach Notification Laws" (2010) < www.ncsl.org > ; *For Your Information* at [51.14].

438 Office of the Press Secretary, United States White House "Fact Sheet: Cybersecurity Legislative Proposal" (12 May 2011) < www.whitehouse.gov > .

439 Department of the Treasury (US) *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

440 EC Directive 2009/136/EC [2009] OJ L337/11.

441 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). For further discussion of data breach notification in Europe see European Network and Information Security Agency *Data Breach Notifications in the EU* (Heraklion, 2011); Article 29 Data Protection Working Party *Opinion 13/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments* (adopted 5 April 2011).

442 Federal Data Protection Act (Germany), s 42a. The German law requires that affected individuals must be notified of any unlawful or unauthorised access of certain categories of personal information if the incident threatens significant harm to the individual.

443 Data Protection Commissioner of Ireland "Personal Data Security Breach Code of Practice" (7 July 2010). This Code implemented one of the recommendations of an independent review focusing on data breach notification: *Report of the Data Protection Review Group* (2010).

444 *For Your Information* at [51.73].

445 Ibid, at [51.51].

446 Asher Moses "Move to Tighten Privacy Rules" *Sydney Morning Herald* (3 May 2011) < www.smh.com.au > .

7.7 No mandatory breach notification laws exist in the United Kingdom, where such laws were rejected by the authors of the *Data Sharing Review Report*[447] and the United Kingdom Government.[448]

7.8 Three Canadian provinces have data breach notification requirements in relation to health information, and Alberta has a notification requirement in relation to unauthorised access to or disclosure of personal information more generally.[449] At the Federal level, a Bill to introduce a mandatory data breach notification requirement to Canada's Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) has been introduced but has not yet passed.[450] 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; the other is issued by the Canadian Privacy Commissioner and applies to PIPEDA.[451]

THE PRESENT NEW ZEALAND LAW

7.9 The Privacy Act, the privacy principles and codes of practice do not currently require 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.[452]

7.10 Failure to notify affected individuals could sometimes be a factor that is taken into account if a complaint is received regarding a breach of principle 5. Principle 5 requires holders of personal information to protect the information by such steps as it is reasonable in the circumstances to take. If an individual were to become aware that his or her own personal information had been compromised, and make a complaint, the Privacy Commissioner could take a failure to notify that individual into account in considering whether the organisation involved took all reasonable steps.[453]

447 The report, commissioned by the UK Government, was 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, 2008) at recommendation 11.

448 Ministry of Justice (UK) *Response to the Data Sharing Review Report* (London, 2008) at 11.

449 Identity Theft Working Group, Uniform Law Conference of Canada – Civil Law Section *Uniform Protection of Privacy Act (Data Breach Notification): Report 2010* (Halifax, Nova Scotia, 2010) at 3.

450 An Act to Amend the Personal Information Protection and Electronic Documents Act (PIPEDA), Bill C-29.

451 Office of the Privacy Commissioner of Canada *Key Steps in Responding to Privacy Breaches* (Ottawa, 2007). The Privacy Act RSC 1985 c P-21 only applies to Canadian public sector agencies. PIPEDA covers private organisations and businesses.

452 See the discussion in *4th Supplement to Necessary and Desirable* at [2.5].

453 See for example *Several People Complain that a Government Department Lost their Personal Information* [2009] NZPrivCmr 16, Case Note 211257. This case note concerns complaints lodged with the Privacy Commissioner after a member of a government agency lost a file on the street. The file contained 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 agency took steps to mitigate any harm that could have resulted from the breach. The agency expediently notified the affected individuals and the Office of the Privacy Commissioner, sought and received legal undertakings from media outlets who obtained the files not to publish the details, and got the original file back with the help of the Police.

The guidelines

7.11 In August 2007, the Office of the Privacy Commissioner (OPC) issued voluntary data breach guidelines – *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* ("the guidelines") – which were finalised and released in February 2008.[454]

7.12 The guidelines go further than advocating notification as a response. They espouse a proactive approach and stress that breach prevention and data security are of prime importance. Notification is one aspect of a wider set of measures aimed at the protection and security of personal information.

7.13 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 disclosed, 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 might be used (particularly whether it might be used for fraudulent or harmful purposes). The organisation should also consider who is affected by the breach, and 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 individual whose personal information has been inappropriately accessed, collected, used or disclosed."[455]

7.14 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. Given their voluntary nature this may never be fully possible.

MANDATORY OR VOLUNTARY NOTIFICATION?

7.15 We asked in our issues paper whether the Privacy Act should contain a mandatory requirement of notification. There was a fairly even split in submissions on this question.

Mandatory notification

7.16 Arguments in favour of a mandatory requirement were set out in the issues paper,[456] and endorsed in some of the submissions. Benefits of notification include:

- Notification can enable the avoidance of further harm. Individuals whose information has been compromised may be able to take steps to mitigate and control the negative effects that can result from a breach. As an obvious example this could involve monitoring bank statements, changing bank account numbers and passwords, or cancelling credit cards. Identity fraud can thus be minimised. Nor are financial harms the only ones against which protective measures might be taken. Stalking, embarrassment, or discrimination can sometimes result from the release or loss of information held by an organisation.

454 Office of the Privacy Commissioner, *Key Steps*, above n 433.

455 Ibid, at 6.

456 Issues Paper at [16.13]–[16.20].

- Individuals have a "right to know" if their information is compromised. They should not be the last to know, for example by reading of the breach in the newspaper (because if it is widespread enough that is probably where it will end up). Earlier notification can enable people to better manage the situation themselves.
- 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".[457] In this regard notification assists in understanding the privacy and security environment and aids the development of policy in this area. It also alerts the community to the prevalence of such incidents.

7.17 Given these benefits, it can be argued that notification should be mandatory. Proper information-handling practices in both the public and private sectors are in everyone's interests. If matters are left to voluntary notification, however, there are incentives not to notify. Notifying individuals in response to a data breach is likely to involve cost, both economic and reputational. There is certainly little incentive to notify in cases where a breach might otherwise remain unknown to the affected individuals or public at large.[458] 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 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 so. Furthermore, a mandatory requirement of notification incentivises attention to, and enhancement of, security arrangements.

Voluntary notification

7.18 The arguments against a scheme of mandatory notification are as follows. They appeared in many of the negative submissions:

- While the minimisation of identity fraud is often put forward as one of the main justifications for a notification regime, one of the few studies on the subject has concluded that the effect of such a regime on the incidence of identity fraud is marginal.[459] There is also little hard evidence that mandatory notification laws have led to a reduction of data breach incidents overall.[460]
- United States privacy law expert Fred Cate has criticised mandatory notifications as "a twentieth century approach to twenty-first century information flows and challenges".[461] He says that in relation to the "bottomless ocean of information",[462] notices are too slow, too cumbersome,

457 Sasha Romanosky, Rahul Telang and Alessandro Acquisti *Do Data Breach Disclosure Laws Reduce Identity Theft?* (Carnegie Mellon University, 2008) at 2.

458 Canadian Internet Policy and Public Interest Clinic *Approaches to Security Breach Notification: A White Paper* (University of Ottawa, 2007) at 23.

459 Romanosky, Telang and Acquisti, above n 457, at 11.

460 Canadian Internet Policy and Public Interest Clinic, above n 458.

461 Fred Cate *Information Security Breaches – Looking Back and Thinking Ahead* (The Centre for Information Policy Leadership, 2008) at 19.

462 Ibid, at 2.

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. Nevertheless Cate's criticism is directed principally at the European Union and United States approaches, and he notes that the detailed New Zealand Guidelines, although voluntary, avoid many of the criticisms he makes; they "reflect many of the practical lessons from the broad and diverse US experience about the advantages and limits of notices".[463]

- Mandatory requirements impose costs and other burdens which are out of proportion to the benefits to the individuals concerned. Indeed, it has been said, sometimes individuals can do nothing about the breach that has happened, and the notification causes them nothing more than unnecessary worry and distress.
- One submitter expressed a view that the obligation to notify can be seen as a punishment. It could also undermine customer trust, and lead to a loss of custom. This, perversely, could act as an incentive to conceal rather than reveal breaches.
- Again perversely, a mandatory requirement could penalise "good players". One writer has said that, as a practical matter, organisations with security policies that are good enough to realise that they have a problem are exposed to much greater liability than organisations that are "truly clueless".[464]

Conclusion

7.19 We have weighed up these competing arguments. We agree that a universal and absolute obligation to notify would be more burdensome than it was worth. Such a system would collapse under its own weight. But it is a question of balance. In particularly serious cases the benefit of notification to affected individuals is so clear that it outweighs the disadvantages to the agency concerned, and those disadvantages will usually not be so great in any case. That will particularly be the case if notification enables the individual to contain or limit the damage, or otherwise to soften the impact. Despite the lack of hard statistical evidence we also think that an obligation to notify can only have a beneficial effect on security systems. Nor do we think that notification necessarily causes reputational damage to an agency. Upfront disclosure of problems can place an agency in a more favourable light than an attempt to cover up which is later exposed in the media, as is by no means unlikely. There will be some cost to agencies, certainly, but provided the obligation to notify is strictly confined to necessary situations, that cost is justified by the benefit to the individuals affected.

7.20 We conclude, therefore, that notification should be mandatory, but only in a clearly confined set of situations.

463 Ibid, at 1.

464 JK Winn "Are 'Better' Security Breach Notification Laws Possible?" (2009) 24 Berkeley Tech LJ 1133 at 1149.

RECOMMENDATION

R67 Data breach notification should be mandatory, but only in clearly confined circumstances.

A SUGGESTED SCHEME

Definition

7.21 The expression "data breach" – if indeed it is that term which is chosen – will need to be defined. In essence we mean by it the unauthorised disclosure of personal information, whether that has occurred as a result of a security breach or unauthorised access, and whether or not that disclosure is attributable to the fault of the holding agency.

Threshold

7.22 It is clear that it would be unworkable to require notification of all breaches. That would be quite unnecessarily costly, and in most cases the benefit would not outweigh the costs. So there should be a threshold for notification, and it should be a reasonably high one. That was supported by a number of submissions. One said that it was crucial to set the threshold at a level which reflects the degree of risk involved in the particular breach.

7.23 One possibility would be to require as a threshold "the likelihood of serious harm resulting from the breach". However, it may sometimes be difficult at the time of the breach for the agency to be able fully to assess the likely degree of harm. We therefore prefer a test with two elements.

7.24 First, there should be an obligation to notify if such notification will enable the recipient to take steps to mitigate a real risk of significant harm. The obvious example would be the case where financial details have been released, and individuals may wish to cancel their credit cards or change their bank account numbers.

7.25 However, this should not be the only criterion. There may be cases, for instance, where particularly sensitive information has been lost, where it is desirable for the individual to have early notification and forewarning of possible consequences. We support, therefore, a second, alternative, criterion that notification should be required if the breach is a serious one. In determining whether or not it is serious, the agency would be required to take into account such matters as:

(a) the degree of sensitivity of the information;
(b) the hands into which it may fall or have fallen;
(c) whether it is reasonably foreseeable that significant harm might result; and
(d) the scale of the breach (for instance, the number of persons affected).

7.26 This is an area where guidelines from the Privacy Commissioner would be very helpful.[465] We would expect the obligation to arise in a minority of cases.

RECOMMENDATION

R68 The criteria for notification should be:

(a) if such notification will enable the recipient to take steps to mitigate a real risk of significant harm; or

(b) if the breach is a serious one.

RECOMMENDATION

R69 In determining whether a breach is serious the agency should take into account:

(a) whether or not the information is particularly sensitive in nature;

(b) the hands into which it may fall or have fallen;

(c) whether it is reasonably foreseeable that significant harm might result; and

(d) the scale of the breach.

Who should notify?

7.27 Generally, the agency which has a direct relationship with the customer should decide whether to notify, and should undertake the notification. Sometimes, however, more than one agency may be involved, and there may be a question of which is the more appropriate. In a case involving credit cards, for instance, there may be a question as to whether the retailer or the bank should bear the responsibility. While doubtless that will usually be resolved by consultation between the two agencies, perhaps with the assistance of OPC guidelines, the legislation will need to prescribe a test for where the responsibility falls. We believe it should lie on the agency which held the information for the purposes of principle 5 and from whose control it has escaped. The duty to notify may be vicariously performed if in a particular case another related agency can do so more easily.[466]

RECOMMENDATION

R70 The responsibility to notify should lie on the agency which held the information for the purposes of principle 5 and from whose control it has escaped.

---

465 The present voluntary guidelines provide:

> 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 individual whose personal information has been inappropriately accessed, collected, used or disclosed. Agencies should also take into account the ability of the individual to take specific steps to mitigate any such harm. There may also be situations where the individual cannot take any steps to mitigate potential harm, but the privacy breach was so material as to warrant notification.

Privacy Commissioner, *Key Steps*, above n 433, at 6.

466 See ibid, at 7.

Who should be notified?

7.28 Individuals whose information has been compromised must obviously be notified. That is the very purpose of the requirement.

7.29 We also think there should be a duty to notify OPC. That office should be told of such matters so as to enable it to build up a statistical record to assist it in performing its other functions. It will be enabled to detect sectors where there may be systemic problems. It may also wish, without disclosing anyone's identity, to notify other traders or bankers about possible criminal activity which has led to the security lapse. The threshold for notifying OPC should be the same as that for notifying the individual. OPC tells us that even now some agencies notify it at an early stage. It should be made clear, however, that OPC should not publish the identities of agencies which notify breaches unless the agencies consent or unless in a particular case the public interest so requires. Otherwise there would be an obvious disincentive to notify. Section 116 of the Privacy Act (the secrecy provision) could be amended to so provide.

RECOMMENDATION

R71 Individuals whose information has been compromised should be notified. The Office of the Privacy Commissioner should also be notified.

RECOMMENDATION

R72 The Privacy Act should provide that the Office of the Privacy Commissioner will not publish the identities of agencies which notify breaches, unless the agencies consent or unless in a particular case the public interest so requires.

Timing

7.30 Notification should be made as soon as reasonably practicable, although there would need to be provision for delay where an investigation by a law enforcement agency is underway which would be prejudiced by publicity. One would hope, however, that this exception would be sparingly used, particularly where the delay would cause prejudice to the potential recipient of the notice.

RECOMMENDATION

R73 Notification should be made as soon as reasonably practicable, with an exception where an investigation by a law enforcement agency might thereby be prejudiced.

Form and content of the notice

7.31 The legislation should not be too prescriptive about content. There is a need to be flexible, so as to meet the circumstances of the case. The notice should be such as to fully and fairly inform the individual, and, where practicable, to point out steps that the individual could take to mitigate loss or harm. The notification should be able to be made by any method, so long as it achieves the objective. Direct notification to the individual is obviously best. When an address is unknown there would need to be provision for substituted service. Where the number of individuals involved is too great to notify each individual separately, a form of public notice may be necessary, although only as a last resort.

RECOMMENDATION

R74 The notice should be such as to fully and fairly inform the individual, and, where practicable, to point out steps the individual could take to mitigate loss.

RECOMMENDATION

R75 Notification should be to the individual where possible, with provision for substituted service.

Exceptions

7.32 We have considered whether there should be any exceptions to the obligation to notify. We do not think that encrypted information should automatically be exempt, but the fact the information was encrypted is a factor which would be relevant in considering the degree of the risk of harm, and therefore whether notification is necessary.

7.33 We also asked in the issues paper about a "public interest" exception. The ALRC recommended that the Australian Privacy Commissioner should have power to waive the notification requirement when notification would not be in the public interest.[467] There was support in submissions for such an exception, but little enthusiasm for OPC being involved in the decision – including from OPC itself. So we recommend that a public interest exception be included, with some examples of the kinds of situation where it would apply, so as to provide as much certainty as possible: national defence and security, and maintenance of the law, would be obvious inclusions. Any agency which wrongly employed this exception would be subject to complaint.

RECOMMENDATION

R76 There should be an exception to the requirement of notification where it would be contrary to the public interest.

467 *For Your Information* at [51.95].

Failure to notify

7.34 If, as we shall suggest, notification becomes part of principle 5, failure to comply would be a ground of complaint to the Privacy Commissioner. Cases might proceed to the Human Rights Review Tribunal where remedies, including damages, might be awarded. If the Privacy Commissioner became aware of a case of non-notification, this might be an instance where the issue of a compliance notice would be merited.[468]

RECOMMENDATION

R77 Failure to notify should be a ground of complaint to the Privacy Commissioner. The Privacy Commissioner should also have power to issue a compliance notice.

The legislative vehicle

7.35 There are several possibilities as to how a mandatory notification requirement might be included in the legislation. We favour it becoming an additional element of principle 5, the security principle, but with more detail contained in specific provisions later in the Act. Principle 6, relating to access to personal information, and the supplemental detail in sections 27–45, is an example of this sort of methodology. Principle 5 is the appropriate principle, in that notification is properly considered as one of the safeguards for security of personal information.

RECOMMENDATION

R78 The obligation to notify should be enacted as part of principle 5, with more detailed provisions elsewhere in the Privacy Act.

Guidance

7.36 In addition to the statutory criteria, we believe that clear explanatory guidance from the Privacy Commissioner will be important. We recommend that, should data breach notification become compulsory, the Privacy Commissioner should publish guidance on the subject. The existing voluntary guidelines should serve as a useful starting point.

RECOMMENDATION

R79 If data breach notification becomes compulsory, the Privacy Commissioner should publish guidance on the subject.

468 See ch 6.

Chapter 8

Interaction with other laws

8.1 The Privacy Act interacts with a number of other statutes and laws. That is neither surprising nor unique. In a non-code system like New Zealand, with a large number of stand-alone Acts, it is inevitable that there will sometimes be questions of how one of those Acts relates to another. But in the privacy arena some of these questions are particularly acute and difficult.

SUBSERVIENCE OF PRIVACY PRINCIPLES TO OTHER LEGISLATION

8.2 Section 7 of the Privacy Act is a ranking provision which confirms that the privacy principles may be modified or overridden by other laws. They must, in other words, be read subject to those other laws. The other laws may either impose stricter requirements than the principles (as for example with the secrecy provisions of some other Acts) or authorise actions which would otherwise breach the principles (as is the case with the Official Information Act).

8.3 However, section 7 is complicated and not user-friendly. The select committee considering the Bill made the decision to bring a number of provisions together into what is now section 7, and by so doing increased its complexity.[469] The section provides:

> **7 Savings**
>
> (1) 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.
>
> (2) Nothing in principle 6 or principle 11 derogates from any provision that is contained in any other Act of Parliament and that
>
> (a) imposes a prohibition or restriction in relation to the availability of personal information; or
>
> (b) regulates the manner in which personal information may be obtained or made available.

469 See the account in the Issues Paper at [11.10], especially n 882–884.

(3) Nothing in principle 6 or principle 11 derogates from any provision

(a) that is contained in any regulations within the meaning of the Regulations (Disallowance) Act 1989 made by Order in Council and in force

(i) in so far as those principles apply to a department, a Minister, an organisation, or a public sector agency (as defined in paragraph (b) of the definition of that term in section 2(1)) that is established for the purposes of assisting or advising, or performing functions connected with, a Department, a Minister, or an organisation, immediately before 1 July 1983; and

(ii) in so far as those principles apply to a local authority or a public sector agency (as so defined) that is established for the purposes of assisting or advising, or performing functions connected with, a local authority, immediately before 1 March 1988; and

(iii) in so far as those principles apply to any other agency, immediately before 1 July 1993; and

(b) that

(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.

(4) An action is not a breach of any of principles 1 to 5, 7 to 10, and 12 if that action is authorised or required by or under law.

(5) Nothing in principle 7 applies in respect of any information held by the Department of Statistics, where that information was obtained pursuant to the Statistics Act 1975.

(6) Subject to the provisions of Part 7, nothing in any of the information privacy principles shall apply in respect of a public register.

8.4 The following matters contribute to the complexity to which we have referred:

- most of the section's provisions are not "savings" provisions at all, so the section heading is misleading;
- principles 6 and 11 are dealt with separately from the other principles;
- even in relation to principles 6 and 11 there is a difference according to whether the other law *authorises* or *restricts* the disclosure of information; and
- one of the provisions relates only to other *Acts*; one to other *enactments*;[470] one to *regulations*; and one to other *law*.

470 By virtue of the Interpretation Act 1999, s 29, "enactment" means "the whole or a portion of an Act or regulations".

8.5 There was a strong call in submissions to our issues paper for section 7 to be simplified. We agree, and recommend that section 7 should be repealed and replaced by a new section. The section should have the heading "Relationship to other enactments". There should be a simple provision that in the case of inconsistency between a privacy principle and another Act, the other Act will prevail. We do not think the detail currently in section 7(1), (2), (3) and (4) is necessary to make the essential message clear. Nor can we see the need to separate principles 6 and 11 from the others as is done in the present section.

8.6 There should be a provision that any regulations already made which prevailed over the privacy principles by reason of the present section 7 should continue to so prevail. However, we do not think that, in future, inconsistent regulations (or other delegated legislation) should automatically prevail over the principles. It is unusual for delegated legislation to be able to modify primary legislation, and it is generally undesirable. It devalues the force of the primary legislation. In an age where concerns about our privacy are increasing, the privacy principles should be seen to be more robust than that. So we recommend that the Privacy Act should contain a provision that, for the future, regulations should not override the privacy principles unless the Act empowering the regulations expressly so provides. A majority of the submissions that addressed this issue supported such a solution.[471]

8.7 There may also be a question of whether the common law can ever override or modify the privacy principles. The implication of the present section 7(4) may be that it can: it uses the words "action authorised or required by or under *law*". Yet it is hard to think of examples where the common law could modify the privacy principles. The new tort of invasion of privacy created by the Court of Appeal in *Hosking v Runting*[472] operates in parallel with, and independently of, the Privacy Act. Moreover, the essentially exclusive jurisdiction of the Privacy Commissioner and the Tribunal over Privacy Act matters reduces any potential significance of the common law in privacy matters. However, there could possibly be instances where a fundamental common law principle may affect the operation of privacy principles. In *QKB & NSN v Commissioner of Police and Chief Executive, Department of Child Youth and Family Services*[473] it was argued that the common law principle of witness immunity should exclude liability for breach of principle 8, but the Tribunal did not need to determine that particular issue. The New Zealand Law Society also gave the example of the common law duty of confidentiality, saying it may apply even though one of the exceptions to principle 11 would otherwise be applicable. We think such situations will be rare. The courts are always open to an argument that an Act is to be read subject to a fundamental common law principle,[474] and we think the Tribunal would take a similar approach were the point ever to arise. We do not think the Privacy Act need make express provision for such a contingency.

471 Section 42A of the Financial Reporting Act 1993 is an example of an express provision allowing delegated legislation to override some privacy principles.

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

473 *QKB & NSN v Commissioner of Police and Chief Executive, Department of Child Youth and Family Services* [2006] NZHRRT 38.

474 See John Burrows and Ross Carter *Statute Law in New Zealand* (4th ed, LexisNexis, Wellington, 2009) at 319–332, 543–558.

8.8 In addition, we recommend that:

- the very specific provision in section 7(5) should be moved to Part 6 of the Act; and
- section 7(6), if it remains necessary in future,[475] would be better located in Part 7 of the Act.

RECOMMENDATION

R80 Section 7 should be repealed and replaced by a new provision. That provision should:

- be headed "Relationship to other enactments";
- provide that in case of inconsistency between a privacy principle and another Act, the other Act will prevail;
- provide that regulations previously made which prevail over the privacy principles should continue so to prevail; and
- provide that in future regulations should not override the privacy principles unless the empowering Act expressly so provides.

RECOMMENDATION

R81 Section 7(5) should be moved to Part 6 of the Act.

RECOMMENDATION

R82 Section 7(6) should be moved to Part 7 of the Act, should such a provision remain necessary.

IMPLIED STATUTORY OVERRIDES

8.9 The most difficult question is whether another statutory provision *impliedly* overrides a privacy principle even though it does not do so expressly. This kind of question is a perennial problem of the New Zealand statute book. A New Zealand textbook on statute law contains a chapter devoted to the question.[476] Sometimes a provision in one Act completely overrides an inconsistent provision in another; sometimes the two can be reconciled by giving one or both a narrow interpretation; sometimes the two can operate in parallel. In the end it is a question of statutory interpretation in each case. The Privacy Act can give rise to such questions.

8.10 Such a problem was confronted by the Tribunal in *Clearwater v Accident Compensation Corporation*.[477] The Tribunal found that, while a provision in the Accident Insurance Act (AIA) 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, the employer's right to receive that information was implicit due to the operation of section 7(1) of the Privacy Act. In other words, the Tribunal found that the AIA impliedly overrode privacy

475 See Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, 2008).

476 Burrows and Carter, above n 474, at ch 14.

477 *Clearwater v Accident Compensation Corporation* [2004] NZHRRT 2.

principle 11. It is not possible to lay down clear rules of interpretation for such a case. Each case has to be treated on its merits. We have considered whether there should be a statutory requirement that, in the case of an apparent inconsistency, the other provision should where possible be interpreted consistently with the privacy principles. Such a provision in the Privacy Act would be akin to section 6 of the New Zealand Bill of Rights Act 1990. But there was not much support for this in submissions, and the Bill of Rights Act experience is not such as to suggest that it would make the interpretive task easier. So we prefer to leave things as they are, with the question of implied statutory override being left to interpretation in each case. The purpose section which we recommend in chapter 2 would serve as an aid to interpretation.

8.11 However, we think there would be merit in inserting in the Legislation Advisory Committee (LAC) Guidelines a guideline that new legislation with privacy implications should, where possible and appropriate, expressly indicate the relationship between the provisions of the Privacy Act and the new Act. The Law Commission recommended similarly in its report on the review of the Land Transfer Act.[478] We also suggest that LAC may wish to re-examine its present guidelines on relationships between Acts to see whether more examples and guidance might be given.[479]

RECOMMENDATION

R83 The Legislation Advisory Committee Guidelines should contain a guideline that new legislation with privacy implications should, where possible and appropriate, expressly indicate the relationship between the Privacy Act and the new Act.

RECOMMENDATION

R84 The Legislation Advisory Committee should consider re-examining its guidelines on relationships between Acts to see whether more examples and guidance might be given.

A LIST OF STATUTORY OVERRIDES

8.12 A number of submitters to the issues paper supported the idea of creating, for the assistance of users, a list of statutory provisions which override or modify the privacy principles. We put forward the possibility that such a list might be included in a schedule to the Privacy Act. However, not only would this be an unusual use of a schedule; there would also be real dangers, in that the judgement on what should or should not be included in the schedule might be open to argument. Nor could the list ever be guaranteed to be exhaustive; it would be too easy to overlook provisions.

478 Law Commission *A New Land Transfer Act* (NZLC R116, 2010) at [5.13].

479 Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2001, most recently amended 2007) at [7.2.1]–[7.2.3].

8.13 It should, however, be possible for the Office of the Privacy Commissioner (OPC) and the Ministry of Justice to prepare a list, at least of the more obvious and frequently arising examples of statutory overrides, as part of the guidance function. Several submitters felt that such a document would be helpful, although again it would need to be made very clear that the list was not exhaustive. We recommend that OPC and the Ministry consider that possibility.

8.14 We proceed now to discuss several interactions of the Privacy Act with other legislation which have given rise to particular difficulty.

RECOMMENDATION

R85 The Office of the Privacy Commissioner and the Ministry of Justice should consider issuing a list of frequently-arising statutory overrides of the Privacy Act.

OFFICIAL INFORMATION LEGISLATION

8.15 The Official Information Act 1982 (OIA) and the Local Government Official Information and Meetings Act 1987 (LGOIMA) provide for the right of individuals to obtain information from government agencies on request. The Acts are based on the premise that such information must be disclosed unless there is good reason for withholding it.[480] The "good reasons" are listed in the Acts. One of them is "the privacy of natural persons", unless in a particular case the privacy reason for withholding the information is outweighed by the public interest in making the information available.[481]

8.16 This importation of "privacy" into the OIA and LGOIMA raises questions about the relationship with the Privacy Act's principles. In our review of the OIA and LGOIMA, on which we shall be reporting later in 2011, we are considering whether there should be some explicit alignment of the concepts of privacy in the Privacy Act and these other two Acts.[482] We shall defer discussion and decision until that report.

8.17 Whatever happens on that question, there was support among submitters for clarifying in the Privacy Act that requests to government agencies for personal information (other than requests by individuals for access to their own information) are governed by the OIA so that the public interest override applies. We recommend that another exception be added to privacy principle 11 (the disclosure principle) making that clear, so as to lessen the confusion which presently sometimes manifests itself. It might read:

> That the disclosure is by a public sector agency and is made in good faith in response to a request under the official information legislation.

480 Official Information Act 1982, s 5; Local Government Official Information and Meetings Act 1987, s 5.

481 Official Information Act 1982, s 9(1), s 9(2)(a); Local Government Official Information and Meetings Act 1987, s 7(1), s 7(2)(a).

482 The matter is discussed in Law Commission *The Public's Right to Know: A Review of the Official Information Act 1982 and Parts 1 to 6 of the Local Government Official Information and Meetings Act 1987* (NZLC IP18, 2010) at ch 6 [*Public's Right to Know*].

8.18 A further difficult question arises as to whether government departments and agencies can use the Official Information Act to obtain personal information about an individual from another government department or agency. This is relevant to the question of information sharing between government agencies which we deal with in appendix 1. We understand that, given some uncertainty about the application of the Privacy Act in that regard, some agencies have contemplated using the OIA route instead. We doubt whether this is permissible. The very purpose of the OIA is to enable "the people of New Zealand"[483] to get information about government and not the reverse. Moreover, the list of persons who can make requests under section 12 of the OIA probably does not include the Crown (although that is not absolutely clear). We are currently disposed to recommend that it be put beyond doubt that the OIA cannot be used for this purpose, but we have sought submissions on the question in our issues paper on the review of the official information legislation,[484] and our final recommendations await our final report on that review.

8.19 We also leave until our report on the official information legislation the resolution of two other issues we raised in our issues paper.[485] The first is whether there should be a complaints process for those affected by the wrongful release of personal information under the OIA and LGOIMA. There was a fair degree of support for such a process in submissions on this issues paper. The other issue, on which submissions were evenly divided, is whether there should be a mandatory consultation process between a public agency and a person who is the subject of personal information in relation to which there is a request for disclosure.

8.20 We also asked for views on whether the current provisions for accessing one's own information should be reconsidered. At present natural persons apply under the Privacy Act, whether the information is held by a public or a private agency, and complaints are dealt with by the Privacy Commissioner. Corporations apply under the OIA where the holding agency is subject to that Act, and complaints are dealt with by the Ombudsmen. The question is whether all access requests to a public agency, whether by corporations or natural persons, should be governed by the OIA. While there is a degree of anomaly in the present position, we point out in the issues paper that any change to the present position would create its own different anomalies.[486] There was no support for change in submissions to the issues paper, and we do not recommend any.

8.21 Finally, we asked whether there was any support for "umbrella" regulation of privacy and official information, perhaps under an information commissioner regime.[487] Few submitters answered this question, and there was not strong support among those who did. We make no recommendations at this stage, although we may revisit the question in our report on the review of official information legislation.

483 Official Information Act 1982, s 4 (the purpose section).

484 Law Commission *Public's Right to Know*, above n 482, at [6.43]–[6.45].

485 Issues Paper at [11.53]–[11.61].

486 Ibid, at [11.75]–[11.78].

487 Ibid, at [11.67]–[11.74].

RECOMMENDATION

R86 An exception should be added to principle 11 making it clear that when requests for personal information are made to agencies subject to the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, the latter Acts govern such requests (except in relation to requests by individuals for access to their own personal information).

PUBLIC RECORDS ACT 2005

8.22 The Privacy Act, the OIA and LGOIMA, and the Public Records Act 2005 (PRA) are the key Acts about the management of information in the public sector. Yet they are administered by different departments, and are less than ideally integrated with each other. There are some ways in which we believe the relationship between the Public Records Act and the Privacy Act could be improved.[488] We discuss three matters.

8.23 First, when public records are transferred to Archives New Zealand, a decision must be made by the head of the controlling public office whether they are to be open access or restricted access records. That decision is to be made after considering, among other things, whether 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.[489]

8.24 Standards have been issued by the Chief Archivist, and they draw attention to the need "to prevent the disclosure of *sensitive* personal information".[490] That is a rather higher threshold than the Privacy Act requires. We are conscious that the documents transferred to Archives are very voluminous indeed. They are measured in metres rather than pages. It would be impossible for anyone to scrutinise them all before transferring them, or accepting transfer of them. So there has obviously to be a classification into categories of document. It would not be realistic to expect exact compliance with principle 11 of the Privacy Act in respect of every page of every document.

8.25 We have wondered whether the PRA should specifically require the Chief Archivist to consult with the Privacy Commissioner during the process of devising standards. This in fact happens anyway, and it is doubtful whether such a statutory direction is necessary. But, given the important relationship between the two pieces of legislation, we think it best to spell it out.

488 We shall consider the relationship between the PRA and the OIA and LGOIMA in our review of the Official Information legislation; see Law Commission *Public's Right to Know*, above n 482, at ch 6.

489 Public Records Act 2005, s 44(1)(a).

490 Archives New Zealand *Making Access Decisions under the Public Records Act: Guidelines for All Public Offices* (2003, revised 2005) at [5.1].

8.26 Secondly, it may be that after material has been placed on open access it is discovered that some items in it contain personal information about an individual which should not properly have been placed on open access: it may indeed be that had the disclosure taken place in any other context it would have been a breach of principle 11. We believe that in such a case the affected person should have a statutory right to request the Chief Archivist to review the decision to place the material on open access. We understand that the Chief Archivist is prepared to undertake such reviews informally now, but we think it would be better to place the right of review on a statutory basis so that all are able to know it exists. In the event that such a review is unsuccessful, we are disposed to think that the aggrieved person should be able to bring a complaint to either the Privacy Commissioner or the Ombudsmen.

8.27 However, we do not make a formal recommendation about this at this stage. A similar question arises if information is wrongly released under the OIA. There is no effective remedy there either, and we ask in our issues paper on the OIA whether there should be. We therefore postpone any formal recommendations about this until our report on the OIA.

8.28 Thirdly, there is an apparent discrepancy between information privacy principle 9 in the Privacy Act and section 18 of the Public Records Act. These provisions both relate to material which is still in the custody of the relevant public office.

8.29 Principle 9 provides:

> *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.

8.30 Section 18 provides:

> **18 Authority required to dispose of public records and protected records**
>
> (1) No person may dispose of, or authorise the disposal of, public records or protected records except with the authority of the Chief Archivist, given in accordance with the provisions of this Act.
>
> (2) Subsection (1) does not apply if the disposal of a public record or a protected record is required by or under another Act.

8.31 The relationship between these two provisions is unclear. In particular it is not clear whether principle 9 is a requirement "under another Act" in terms of section 18(2). This confusion should be removed by making it express which of these two provisions prevails. We think that section 18 should be the dominant provision. It relates to the maintenance of records by a public office. If those records contain personal information, information privacy principle 11 of the Privacy Act, and the privacy withholding ground in the OIA and LGOIMA, should provide adequate protection as long as they continue to be held by the agency. We believe a subsection should be added to section 18 of the PRA spelling out that section 18 prevails over principle 9.

RECOMMENDATION

R87 The Public Records Act 2005 should require the Chief Archivist to consult the Privacy Commissioner when preparing standards about access to archived records.

RECOMMENDATION

R88 A subsection should be added to section 18 of the Public Records Act expressly providing that that section prevails over principle 9 of the Privacy Act.

CRIMINAL DISCLOSURE ACT 2008

8.32 In chapter 9 on law enforcement we discuss the relationship between the Privacy Act and the Criminal Disclosure Act (CDA). The Police are concerned that the confined scope of the CDA still leaves room for the application of the Privacy Act, and that there should be an amendment narrowing the rights of individuals to access information. We think the problem is largely a transitional one, and that with the passage of time the CDA will increasingly cover the territory. We explain our views on this issue more fully in chapter 9.[491]

8.33 However, there is a further issue in the relationship between the Privacy Act and the CDA which is more appropriately discussed in this chapter. Section 16 of the CDA provides grounds on which a prosecutor may withhold information to which a defendant would otherwise be entitled. They include (among a long list) situations where disclosure is likely to endanger the safety of any person, or to facilitate the commission of another offence, and where the information reflects on the credibility of a possible defence witness. Section 17 prohibits the disclosure, without leave, of the address of a witness. Section 18 provides for the withholding of information which would disclose a trade secret or would be likely to unreasonably prejudice the commercial position of a person.

8.34 An omission from the list is the situation where disclosure of the information would involve the unwarranted disclosure of the affairs of another individual. There is such a withholding ground in section 29(1)(a) of the Privacy Act, a section dealing with access to one's own information. No doubt disclosure under the CDA often needs to include information about the victim of the alleged offence, even where that information is of a highly personal nature. We are concerned with the case where the information relates to the personal affairs of *other* persons, and we wonder whether there should be a withholding ground which mirrors that in the Privacy Act.

491 See [9.26]–[9.31].

8.35 Our attention was drawn to this gap in the Act by the submission by Trade Me to our issues paper. They described a case, which attracted wide media publicity at the time, where some 3,000 Trade Me members' contact and trading details had ended up in a Mount Eden jail cell.[492] The information had been obtained by Police for law enforcement purposes. The prosecutors apparently felt the CDA required them to disclose details of those 3,000 innocent parties to the accused. We have considered what can be done to improve matters.

8.36 It may be that part of the problem in this case lay with the breadth of the Police's warrant. Be that as it may, it does seem unsatisfactory that the CDA does not address this situation. We are sympathetic to the argument that sometimes there is such a volume of material that it would be impractical to require an assessment of every page of it before disclosure is made. But matters affecting the privacy of an individual are no more susceptible to that argument than any other of the items in the withholding provisions in sections 16–18: the trade secrets exception, for example, or that relating to the facilitation of the commission of another offence. We note also that other provisions of the CDA (sections 29(3)(c) and 29(4)) do recognise a privacy interest.

8.37 However, there is an argument that this new withholding ground is unnecessary, for the reason that the prosecution's only duty under the CDA, section 13, is to disclose "relevant" information. Information about "another individual" will not usually be relevant. More than this, an "unwarranted" disclosure of information is by definition an irrelevant disclosure. There is an element of tautology in employing both concepts in the same provision. Yet we believe, as a result of the Trade Me case, that it would be desirable for the CDA to make specific reference to the interests of other individuals, as a signal of the importance of privacy rights. To avoid the tautology to which we have just referred we suggest that, rather than adding a new withholding ground, a new provision be inserted in section 16 of the CDA to the effect that, in deciding whether information is relevant for the purpose of section 13(2), consideration must be given to the extent to which it relates to the private affairs of another individual.[493]

RECOMMENDATION

R89 Section 16 of the Criminal Disclosure Act 2008 should contain a provision that, in deciding whether information is relevant for the purpose of section 13(2) of that Act, consideration must be given to the extent to which it relates to the private affairs of another individual.

492 See Anna Leask "Police Deliver TradeMe Names to Prisoners" *New Zealand Herald* (Auckland, 3 August 2008) < www.nzherald.co.nz > ; "TradeMe Details Handed to Prisoner" (3 August 2008) < www.stuff.co.nz > .

493 We leave out of account the question of whether, if sensitive personal information about another individual were to be disclosed, there could be a complaint to the Privacy Commissioner for the breach of principle 11. Perhaps there could: section 42 of the CDA provides that nothing in the CDA affects any provision of any other enactment that imposes a restriction in relation to the availability of information.

EVIDENCE REGULATIONS 2007

8.38 There is a question about an interrelation between the Privacy Act and the Evidence Regulations 2007. These Regulations apply to a video record when it is intended that the record may later be offered by the prosecution as evidence in criminal proceedings. They contain detailed provisions for the recording and retention of the video record, and also for access to the record. They provide for a master copy and working copy to be made. The master copy must be produced at a criminal proceeding, and then retained in the custody of the court until the prescribed destruction date. The working copy may only be shown by the Police to the persons, and for the purposes, specified in regulation 20.[494]

8.39 The Police have queried whether these Regulations override the Privacy Act. If they do not, persons the subject of a video could seek access to it under principle 6 of the Privacy Act. Given the care with which access rights have been spelt out in the Evidence Regulations, we think the clear intention is that those Regulations prevail over the Privacy Act. This override of the Act by Regulations is probably permitted by the current s 7(1) of the Privacy Act.[495]

8.40 The conclusion that the Evidence Regulations are meant to be predominant is strengthened by regulation 37, which emphasises that the video record is to be kept in a way that preserves the privacy of the persons recorded on it.

8.41 Given the doubts that have arisen about this, we believe that the Evidence Regulations should expressly provide that they apply to the exclusion of the access and correction provisions of the Privacy Act, namely principles 6 and 7.

---

494 The full text of reg 20 is as follows:

20 Limited purposes for which Police may show working copy

The Police may only show a working copy for the following purposes:

(a) to seek advice from a lawyer or any other person to determine whether –

(i) any, and if so what, charges ought to be laid; or

(ii) any care or protection proceeding ought to be instituted:

(b) to allow any of the following persons to know the case against them:

(i) a person suspected of having committed an offence to which the video record relates;

(ii) a defendant to any charge laid in relation to which the video record may be used in evidence;

(iii) an accused against whom an indictment has been filed in relation to which the video record may be used in evidence:

(c) to allow any lawyer representing any person referred to in paragraph (b) to view it:

(d) to allow the witness to view it:

(e) for the purpose of making a transcript:

(f) to allow any lawyer representing the witness or the Crown to view it:

(g) to enable any Judge to view it in order to –

(i) determine whether it is admissible in a proceeding; or

(ii) comply with any requirement in an enactment or imposed by a rule of law:

(h) to enable the Commissioner or any other member of the Police to discharge his or her duties under an enactment:

(i) to assist the Police in any further investigations of suspected offences that may have been committed by any person referred to in paragraph (b).

495 This is on the assumption that it "*authorises*" personal information to be made available. If it imposes a *restriction* on availability under s 7(2) it would be different, because that subsection only applies to *Acts*, not regulations. See the discussion of the complexities of s 7, above.

8.42 We note that there is also a question of the interrelationship of the Evidence Regulations and the Criminal Disclosure Act 2008. Section 42(2) of the latter Act provides:

> (2) Without limiting subsection (1), nothing in this Act applies in respect of any videotape made under the Evidence (Videotaping of Child Complainants) Regulations 1990 or any copy or transcript of such a video (as that term is defined in those regulations).

8.43 However, the Evidence (Videotaping of Child Complainants) Regulations 1990 were revoked by the Evidence Regulations 2007. Section 42(2) should be amended to refer to the current regulations. They are wider, and thus cover more territory, than the 1990 regulations, but their scheme and purpose would seem to require that they override the Criminal Disclosure Act, just as we have concluded that they override the access provisions of the Privacy Act.

RECOMMENDATION

R90 The Evidence Regulations 2007 should expressly provide that they apply to the exclusion of privacy principles 6 and 7.

RECOMMENDATION

R91 Section 42(2) of the Criminal Disclosure Act 2008 should be amended to refer to the Evidence Regulations 2007.

CRIMINAL PROCEEDINGS (ACCESS TO COURT DOCUMENTS) RULES 2009

8.44 The relationship between the Privacy Act 1993 and the Criminal Proceedings (Access to Court Documents) Rules 2009 also merits discussion.

8.45 Concerns have been expressed to us that sometimes these two enactments can provide alternative routes to obtaining the same documents. A defendant or some other person associated with the proceeding may, rather than requesting access to documents on the court file, ask the Police for them under principle 6 of the Privacy Act. (As the Criminal Disclosure Act 2008 comes, with time, to cover more of the ground, this possibility will lessen: it is largely a transitional problem.) In the meantime there would seem to be nothing contrary to principle in what is happening. The Rules apply only to documents "while they are in the custody or control of the court".[496] No breach of the law is committed by a person who obtains the information from another source.[497] In cases where access to the court record has been prohibited by the court, the "maintenance of the law" or contempt of court withholding grounds in sections 27(1)(c) and 29(1)(i) of the Privacy Act would normally be adequate to justify withholding. We do not think any amendment is necessary to deal with this matter.

496 Criminal Proceedings (Access to Court Documents) Rules 2009, r 4(1).

497 See *Hunt v A* [2007] NZCA 332, [2008] 1 NZLR 369 at [53]–[54].

8.46 In the issues paper we asked submitters for their views on issues relating to the Health and Disability Commissioner Act 1994, the Statistics Act 1975 and statutory secrecy provisions.[498]

Health and Disability Commissioner Act 1994

8.47 Currently the Health and Disability Commissioner (HDC) can deal with complaints about patient privacy, but not in relation to *information* privacy: that is the province of the Privacy Commissioner. We noted in our issues paper that the HDC has submitted that the distinction is artificial and unsatisfactory, and has recommended that the two Commissioners should have joint jurisdiction over information privacy complaints in the health sector.[499] The Privacy Commissioner disagreed. We sought comment in the issues paper. Few submitters to our issues paper commented on this issue. IHC supported the HDC recommendation, while 3 submitters and OPC supported the status quo.

8.48 We understand that the HDC and the Privacy Commissioner are working on a Memorandum of Understanding on jurisdictional issues. We support that initiative, and see no need to make any recommendation on this matter.

Statistics Act 1975

8.49 The issues paper asked about privacy protection for personal information used for official statistical purposes.[500] Statistics New Zealand submitted that the Statistics Act already provides an acceptable framework. The submission also noted that work on development of a code of practice for data integration (something that was mentioned in the issues paper) is not presently a priority, given the specialist resources that would be required.

8.50 A range of comments was received from other submitters. These included support for a code of practice (Commerce Commission); noting the limits of depersonalisation and anonymisation which are relied on to protect privacy in the statistical use of personal information (OPC and Privacy Officers' Round Table); and advocating freer access to statistical information by researchers, balanced by very high standards of data security (Department of Corrections).

8.51 One legislative development since release of the issues paper is a proposed amendment to the Statistics Act to allow the release of statistical information held by the Government Statistician to any person for bona fide research or statistical purposes in relation to a matter of public interest.[501] (Currently, official statistical information may only be released to officers of government departments.)[502]

498 Issues Paper at [11.97]–[11.108].

499 The Minister of Health did not agree to the Health and Disability Commissioner's recommendation: Letter from Hon Tony Ryall to Health and Disability Commissioner regarding the Review of the Health and Disability Commissioner Act 1994 and Code of Health and Disability Services Consumers' Rights (23 September 2010).

500 Issues Paper at [Q141].

501 Regulatory Reform Bill 2010 (269–1), cl 107, amending Statistics Act 1975, s 37C.

502 Statistics Act 1975, s 37C.

8.52 Proposed safeguards in the amending clause include deletion of name and address information prior to disclosure, a statutory declaration of secrecy by the researcher, and the Government Statistician being satisfied that the security of the information will not be impaired. Researchers may only use the information for the purposes of their research or statistical project and must comply with any directions given by the Statistician. Failure to comply with these requirements would be an offence.

8.53 We have not received sufficient support in submissions to make any particular recommendation about the protection of personal information used for official statistical purposes.[503] However, the potential for personal information to be used for statistical purposes by a broader range of researchers than in the past means that this is an issue that should be kept under review. Development of a code of practice may be desirable as a means of ensuring adherence to appropriate privacy standards. In the absence of a code of practice, the Government Statistician can give directions as to the handling of statistical information, which could include compliance with any relevant policy or protocol.

Secrecy provisions

8.54 We asked whether a review of statutory secrecy provisions would be desirable, noting that such a review has been undertaken in Australia.[504] There was some support for a review amongst the few submitters who addressed the question, although the Department of Internal Affairs suggested that these provisions should be reviewed on a case-by-case basis by the relevant agency as part of the regulatory scanning process across the state sector.

8.55 We do not support a comprehensive review: such an expenditure of resources is not, we think, justified at this time. However, we recommend that secrecy provisions be included in the list of overriding provisions that we suggest be prepared by OPC and the Ministry of Justice.[505] The matter should also be addressed in the enhanced discussion of relationships between Acts in the LAC Guidelines, which we have recommended above.[506]

8.56 In an earlier report we have also recommended that at such time as statutes imposing a criminal penalty for disclosing information are reviewed, the review should address the question of whether the offence provision is necessary, or whether the Privacy Act provides adequate protection, and that attention should be paid to consistency with analogous provisions.[507] Secrecy provisions that impose a criminal penalty for disclosure of personal information would fall within the scope of this recommendation.

503 Note however that in ch 3 we do make some recommendations about exceptions relating to statistical information, see R13 and R33.

504 Issues Paper at [Q142]; Australian Law Reform Commission *Secrecy Laws and Open Government in Australia* (ALRC R112, Sydney, 2010).

505 See R85.

506 See R83–R84.

507 Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, 2010) at R30, R31.

RECOMMENDATION

R92 Statutory secrecy provisions should be addressed in:

(a) the list of provisions overriding the privacy principles that we suggest be prepared by the Office of the Privacy Commissioner and the Ministry of Justice (R85); and

(b) the enhanced discussion in the Legislation Advisory Committee Guidelines of relationships between Acts (R83 and R84).

Chapter 9
Law enforcement

9.1 In the issues paper, we asked questions about the operation of the Privacy Act in the context of law enforcement. Law enforcement interests intersect with and may override privacy values in two distinct ways:

- They may override privacy access rights by requiring the withholding of information that an individual would otherwise expect to be able to access about themselves under principle 6, if providing access would undermine law enforcement objectives.
- They may override privacy principles which would otherwise apply as to the collection, use or disclosure of information about an individual where this may be required on law enforcement grounds.

The law enforcement overrides in each case take the form of an exception to the relevant privacy principle on the ground of avoiding prejudice to the "maintenance of the law". While the overrides take a similar form, there is a conceptual difference depending on context. In the case of access under principle 6, the override is restrictive as it suppresses access to someone's own personal information, while in relation to the other principles where it applies, the override is permissive as it allows actions such as disclosure that would not otherwise be permitted.

9.2 Our inquiry has examined the law enforcement overrides from these two perspectives. Our primary focus has therefore been on:

- law enforcement and criminal disclosure grounds for refusing access requests;[508] and
- law enforcement grounds for disclosing and sharing personal information, including both the disclosure principle (privacy principle 11), and the information sharing framework for law enforcement information contained in Part 11 and Schedule 5 of the Privacy Act.[509]

508 Issues Paper at 327–333.

509 Ibid, at 333–344.

Should the maintenance of the law access refusal ground be redrafted?

9.3 Sections 27 to 29 of the Privacy Act set out various grounds on which requests by individuals for access under principle 6 to personal information held about them by an agency can be refused. One of these allows any agency, including a law enforcement agency, to refuse access if disclosure of the information would be likely:[510]

> to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial.

9.4 In the issues paper, we asked about the structure of this access exception, in particular whether it would benefit from being expressed in more specific terms,[511] noting alternative formulations of the provision in other jurisdictions and an earlier recommendation of the Privacy Commissioner that consideration be given to making plainer through redrafting the protected constituent law enforcement interests.[512] We also asked whether it would be helpful for the Privacy Commissioner to provide information or commentary about this refusal ground.[513]

Submissions

9.5 There was notable support in submissions for a more specific provision; however, there was also a measure of support for retaining the current provision or using other measures to achieve greater clarity. Areas that submitters suggested needed clarification in particular were (i) the protection of informants and the anonymity of people making confidential allegations; and (ii) the protection of information relating to investigations. The Ministry of Social Development informed us that it can be difficult to convince potential informants that section 27(1)(c) applies to protect their identity and that the lack of a guarantee of confidentiality means that allegations may be made anonymously, which makes it difficult to follow up or investigate the allegations thoroughly.

9.6 The Police noted that if the provision was made more specific, they would need to retain the discretion to rely on a generic refusal ground, so that, for example, they would not have to specifically disclose that access was being refused to protect an informant, in case the disclosure of the basis for the refusal itself prejudiced the maintenance of the law.[514]

510 Privacy Act 1993, s 27(1)(c).

511 Issues Paper at [Q144].

512 *Necessary and Desirable* at recommendation 48.

513 Issues Paper at [Q145].

514 Section 32 of the Privacy Act allows agencies to give notice neither confirming nor denying the existence of information sought under access requests, if disclosure would prejudice the maintenance of the law. Section 44 of the Privacy Act allows agencies the option of declining to provide grounds supporting reasons for refusal if identifying those grounds would itself prejudice the interest protected by the refusal ground.

9.7 In their responses to the issues paper, the Ombudsmen and the Privacy Commissioner noted that the provision is not unique to the Privacy Act as it is also used as a ground to withhold information in the official information statutes (whether under an official information request or under an access request)[515] and in the Criminal Disclosure Act 2008.[516]

9.8 Trade Me suggested that the threshold for refusing access to avoid prejudice to the maintenance of the law should be made consistent with the threshold for reliance on the maintenance of the law exception to principle 11. Access may be refused where prejudice to the maintenance of the law would be likely, whereas disclosure may be made under principle 11 where an agency believes on reasonable grounds the disclosure is necessary to avoid prejudice to the maintenance of the law. Trade Me pointed out that this structural difference can create difficulties where agencies respond to requests for disclosure from law enforcement agencies, and then receive access requests relating to those law enforcement disclosures. In this situation, it may not be clear to an agency whether complying with an access request would prejudice the maintenance of the law; however, advice from the law enforcement agency may provide reasonable grounds to refuse the access request.

9.9 Submissions showed strong support for Privacy Commissioner guidance about the access refusal ground. One law enforcement agency suggested that information in a similar form to that provided by the Australian Privacy Commissioner[517] would be useful, and that further detail would assist agencies and requesters to apply the provision.

9.10 The Ombudsmen and the Privacy Commissioner suggested that any guidance should be coordinated between themselves and the Ministry of Justice and should cover the use of the provision across the Privacy Act, the official information statutes and the Criminal Disclosure Act.

Our response

Redrafting

9.11 Although the phrase "maintenance of the law" is commonly used in legislation, its precise meaning is not always clear.[518] The Privacy Commissioner acknowledged to us that the phrase has become a term of art, although it is considered to generally work reasonably well. The Privacy Officers' Roundtable described it as "a rather tortuous expression." Using tools of statutory interpretation, its main focus is the criminal law; however, the provision is expressed sufficiently broadly to apply in a wide range of contexts, including civil matters and investigations. It is not specifically limited to maintenance of

515 Official Information Act 1982, s 6(c), s 27(1)(a); Local Government Official Information and Meetings Act 1987, s 6(a) and s 26(1)(a).

516 Criminal Disclosure Act 2008, s 16(1)(a).

517 Privacy Commissioner (Australia) *Information Sheet Private Sector 7 on Unlawful Activity and Law Enforcement* (Sydney, 2001) < www.privacy.gov.au > .

518 See also Law Commission *The Public's Right to Know: A Review of the Official Information Act 1982 and Parts 1 to 6 of the Local Government Official Information and Meetings Act 1987* (NZLC IP18, 2010) at [7.29] [*Public's Right to Know*].

the law by law enforcement agencies, or even, in the case of the Privacy Act access refusal ground, to maintenance of the law by public sector agencies. However, the extent to which the provision can operate to protect against prejudice to the maintenance of the law by other agencies is not clearly defined.

9.12 Any reform of the maintenance of the law provision needs to be mindful of the different legislative contexts in which it is used. As we noted in the review of the official information legislation, the same solution may not be appropriate in each case.[519] The balance of interests in each statute may dictate that a different emphasis will need to be reflected in the drafting. Where the provision is used permissively to allow certain actions to avoid prejudice to the maintenance of the law (for example, as exceptions to principles 2, 3, 10 and 11) it may be appropriate for the provision to take a different form.[520] However, a reasonably consistent statutory formulation across legislation is likely to be appropriate where the maintenance of the law provision is used as a ground to withhold information.

9.13 Having assessed the difficulties with the maintenance of the law access refusal ground, we think that it is unlikely that significant improvements can be made through extensive redrafting. We think that much of the difficulty with the provision could be addressed by guidance and commentary from the Privacy Commissioner. We discuss the need for guidance below. However, one necessary amendment to section 27(1)(c) is to clarify that the ground is concerned with protecting the maintenance of the law by public sector agencies (as is the parallel exception in principle 11). In response to the Trade Me submission, we also recommend an amendment to make the threshold for application of the access refusal grounds consistent with the threshold for application of the exceptions to principle 11.[521]

9.14 We have asked submitters for their views about the maintenance of the law withholding ground in an issues paper about the review of the official information legislation.[522] We are in the process of analysing submissions. Should we conclude that amendments should be made in response to those submissions, it may be that parallel amendments would need to be made to section 27(1)(c) of the Privacy Act. We will reach final conclusions about the need for any further redrafting in our forthcoming report on the official information legislation.

RECOMMENDATION

R93 Section 27(1)(c) should be amended to clarify that the access refusal ground is concerned with protecting the maintenance of the law by public sector agencies.

519 Ibid, at [7.38].

520 For example, the right to a fair trial is included in s 27(1)(c), but is not expressly mentioned in the maintenance of the law disclosure exception in principle 11(e), while the disclosure exception includes other grounds such as enforcement of pecuniary penalties, protection of the public revenue and the conduct of judicial proceedings.

521 See R21.

522 Law Commission *Public's Right to Know*, above n 518, at [Q30].

New withholding ground for information relating to investigations

9.15 The status of information relating to investigations was one of the issues raised in submissions to the privacy review. In our issues paper on the review of the official information legislation, we have proposed a new withholding ground to cover material provided in the course of inquiries and investigations, as follows:[523]

> if the withholding of the information is necessary to protect information which has been provided to a department or organisation in the course of an investigation or inquiry and disclosure is likely to prejudice the conduct or outcome of that investigation or inquiry.

In the context of the official information legislation this would not be a conclusive withholding ground, and it could be outweighed if public interest factors are sufficiently important to justify disclosure.

9.16 Our current view is that if this ground is added to the official information legislation, it would also be useful to clarify this matter in the Privacy Act, to make clear that information relevant to a current investigation or inquiry can be protected if its release would prejudice the investigation. However, we have not yet reached a final conclusion about this and are in the process of considering submissions on the proposal. We will therefore make a final recommendation about this in our forthcoming report on the official information legislation.

9.17 The remaining question is whether an additional withholding ground should be included in the Criminal Disclosure Act as well. However, we are satisfied that this would not be necessary. The public interest justification for protecting information subject to an investigation could not be expected to override a defendant's interest in receiving all relevant information relating to criminal charges.[524]

9.18 Some submissions suggested that consideration be given to whether information relevant to investigations should be protected beyond the conclusion of an investigation, to avoid the risk of jeopardising flows of information that assist investigative or enforcement functions.

9.19 Where the investigation is a criminal one, our view is that the maintenance of the law provision may provide grounds for protecting information the disclosure of which would otherwise have a chilling effect on the provision of informant information for enforcement purposes. While this would not necessarily apply in the case of non-criminal investigations, there is likely to be a lesser public interest in denying access in this context. We are satisfied that it is unnecessary to specifically address the withholding of information following the conclusion of an investigation.

523 Ibid, at [7.36].

524 One withholding ground in the Criminal Disclosure Act 2008 (s 16(1)(k)) is where disclosure would be contrary to the provisions of any other enactment. This may apply to investigatory material depending on the legislation applicable to the particular agency, such as a secrecy provision.

Protecting informants

9.20 The other specific area that submissions noted for reform was clarification of the protection of the anonymity of informants. Professor Roth has summarised the position about access to the identity of informants in *Privacy Law and Practice*.[525] Decisions of the Complaints Review Tribunal have confirmed that while identity information about informants is considered to be personal information about the person being informed upon, identity information may be suppressed under section 29(1)(a) (unwarranted disclosure of the affairs of another person) or section 27(1)(c) (maintenance of the law). However, there is no blanket rule protecting all information supplied to the Police and no automatic right to withhold information of that kind. Whether such information can be withheld depends on the circumstances of the case.[526] One Tribunal decision noted that:[527]

> Section 27(1)(c) [of the] Privacy Act provides agencies like the defendant (e.g. Child, Youth and Family, the police) which rely on the free flow of information from informants to carry out their statutory functions of investigating and detecting offences with the means to ensure that the identity of informants will be kept confidential. If they could not do so their sources of information would dry up and they would be hindered in the performance of these functions.

9.21 On appeal, the High Court commented:[528]

> There is … a substantial body of decisions dating from 1982 which have recognised that in a proper case, s 27(1)(c) may be relied on to deny access to the name of an informant. The decisions are firmly grounded in the words of the statute and in the pragmatic concerns which, since *R v Hardy* (1794) 24 St Tr 199, have conferred public interest immunity on police informants. For more than two centuries it has been accepted that the public interest favours preserving the anonymity of police informers by keeping open avenues of information which will assist in the detection and investigation of crime.

9.22 Professor Roth notes a number of Privacy Commissioner case notes where informant identity information was found to have been appropriately withheld because the authority concerned relies on the free and unsolicited flow of information, which is in the public interest and crucial to an authority's law maintenance function.

9.23 On the basis of the series of decisions reviewed by Professor Roth, our view is that the existing access refusal grounds are adequate to protect the identity of informers in appropriate cases. However, the fact that this issue was raised in submissions indicates that this is an area in which Privacy Commissioner guidance may assist. The Privacy Commissioner's website has commentary on the maintenance of the law withholding ground that includes information responding to frequently asked questions, such as "Can I find out who gave information against me?" and "What if an informant provided false information

525 Paul Roth *Privacy Law and Practice* (looseleaf ed, LexisNexis) at [PVA27.7(d)].

526 *Director of Human Rights Proceedings v Commissioner of Police* HRRT 34/05, 6 November 2007.

527 *Nicholl v Chief Executive of Work and Income* CRT 13/01, 31 August 2001 at [5].

528 *Nicholl v Chief Executive of Work and Income* HC Rotorua, AP255/01, 6 June 2003 at [16].

in order to get me into trouble?", as well as links to relevant case decisions.[529] The information is a fairly general summary as it is intended to assist people seeking access to their information under principle 6 to understand the relevant provisions, as well as agencies who respond to these requests. The Privacy Commissioner may wish to consider making more detailed supplementary information on this point available for agencies.

A need for guidance

9.24 Submissions demonstrated that agencies find the maintenance of the law access refusal ground difficult to apply and there was a clear demand for more developed information or guidance. We recommend that the Ministry of Justice coordinate the development of guidance or commentary on this provision by the Ministry, the Ombudsmen and the Privacy Commissioner. The commentary or guidance should cover use of the provision in the Privacy Act, the official information legislation and the Criminal Disclosure Act.

9.25 If it is not possible to produce coordinated guidance in the short term, we recommend that the Privacy Commissioner develop independent guidance on the maintenance of the law access refusal ground in the Privacy Act in consultation with the Ministry of Justice and the Ombudsmen. We consider guidance in this area to be a high priority, based on the response in submissions, and the fundamental importance of the relationship between law enforcement objectives and privacy rights.

RECOMMENDATION

R94 The Ministry of Justice should coordinate with the Privacy Commissioner and the Ombudsmen on the development of guidance or commentary on the maintenance of the law as a ground to refuse or withhold the provision of information. The commentary or guidance should cover use of the provision in the Privacy Act, the official information legislation and the Criminal Disclosure Act.

RECOMMENDATION

R95 Should it not be possible to produce coordinated guidance in the short term, the Privacy Commissioner should develop independent guidance on the maintenance of the law access refusal ground in the Privacy Act in consultation with the Ministry of Justice and the Ombudsmen.

529 Office of the Privacy Commissioner "Maintaining the Law" < http://privacy.org.nz/maintaining-the-law > .

Is the criminal disclosure access refusal ground adequate?

9.26 We asked a specific question about the inter-relationship between the Privacy Act access provisions and the Criminal Disclosure Act 2008.[530] The Criminal Disclosure Act codifies in legislation the disclosure obligations of the prosecution and the defence in criminal proceedings. As a consequence, the Privacy Act was amended to include an additional ground for refusing access requests:[531]

> (ia) the request is made by a defendant or a defendant's agent and is –
>
> (i) for information that could be sought by the defendant under the Criminal Disclosure Act 2008; or
>
> (ii) for information that could be sought by the defendant under that Act and that has been disclosed to, or withheld from, the defendant under that Act.

The new refusal ground allows agencies to consider the question of the disclosure of information relating to criminal proceedings under the Criminal Disclosure Act, to the exclusion of the Privacy Act access provisions.

9.27 The Criminal Disclosure Act also repealed section 31 of the Privacy Act which provided for access to offence-related information to be denied to any person who had been imprisoned for that offence. Section 31 had never been brought into force before its repeal.

Submissions

9.28 The Police submitted that the Criminal Disclosure Act does not fully deal with the issue of access requests to law enforcement agencies that relate to criminal proceedings. This is because the Criminal Disclosure Act does not apply to requests for information that relate to proceedings that predate the legislation.[532] Another limitation is that the Criminal Disclosure Act applies once criminal proceedings have been commenced. Information requests made before the commencement of criminal proceedings therefore have to be dealt with under the Privacy Act.

9.29 A particular concern for law enforcement agencies is the disclosure of sensitive offending-related information (particularly information about sexual or violent offences) that may then circulated inappropriately by the offender within the prison environment, potentially adding further distress to the victims of such offences and their families. In chapter 3, to address this concern, we recommend a specific new ground for refusing access to information that relates to offending which would be likely to cause significant distress to the victim or the family of a deceased victim.[533] We also recommend a new ground for refusing access where the disclosure would create a significant risk of serious harassment of an individual.[534]

530 Issues Paper at [Q146].

531 Privacy Act 1993, s 29(1)(ia).

532 The Criminal Disclosure Act 2008 came into force in 2009.

533 See R25.

534 See R23.

9.30 The Department of Corrections suggested that another part of the solution is to educate defence counsel about the inappropriate circulation of defence material within prisons. Another option suggested by the Department was to set aside a secure room for case preparation so that access to sensitive material can be provided through inspection, rather than by providing copies of the material requested.[535]

Our response

9.31 Apart from the new refusal grounds we recommend in chapter 3, we do not recommend any further legislative measures that would limit access by offenders to information about them or their offending. The Criminal Disclosure Act is still relatively new. There will be a backlog of requests that will have to be worked through under the Privacy Act access provisions. In future, however, such requests can be streamlined under the criminal disclosure process. In the meantime, the Privacy Act provides a framework to deal with residual requests, with various exceptions that can be used to refuse access in appropriate cases. The Privacy Act should also continue to provide a framework to deal with requests that fall outside the criminal disclosure framework.

INFORMATION DISCLOSURE AND INFORMATION SHARING

9.32 We now discuss the law enforcement override of privacy principle 11. This principle places limits on the disclosure of information, subject to a number of exceptions, including an exception where the restriction on disclosure would prejudice the maintenance of the law:

> 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, –
>
> …
>
> (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).

9.33 In this context the override is permissive as it permits, on law enforcement grounds, the disclosure of information about a person that would otherwise be restricted.

9.34 In the issues paper we described the grounds on which the Privacy Act allows for the disclosure and sharing of information for law enforcement purposes, in particular the maintenance of the law exception to principle 11, and the law enforcement information sharing framework in Schedule 5.[536]

535 See Privacy Act 1993, s 42.

536 Issues Paper at [12.22]–[12.26], [12.40]–[12.44], [12.54]–[12.55].

Principle 11 and the maintenance of the law exception

9.35 Questions we asked about the maintenance of the law disclosure exception paralleled those we asked about the maintenance of the law access refusal ground; namely whether the maintenance of the law disclosure ground needs any legislative amendment to provide greater clarity[537] and whether it would be helpful for the Privacy Commissioner to provide information or commentary about the provision.[538] We also asked whether there should be separate maintenance of the law disclosure exceptions, depending on whether disclosure is by a law enforcement agency or to a law enforcement agency,[539] and whether there needs to be greater clarity about information sharing between law enforcement agencies for law enforcement purposes.[540]

Submissions

9.36 There was a reasonable degree of support for reforming the maintenance of the law provision as it is used in principle 11, although a number of agencies support the current provision. There was also notable support for commentary or guidance from the Privacy Commissioner about the exception.

9.37 Among submitters who responded to the question, there was support for the proposal for 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. However, other submitters felt it was unnecessary to restructure the exception in that way as the current provision is considered to provide case-by-case flexibility. Trade Me noted that the factors in determining each kind of disclosure to be "necessary" are different, and so distinguishing the different disclosure contexts could be useful. The Police also believe that it would assist agencies if the maintenance of the law provision was separated into categories in order to reduce confusion. One agency suggested that it would be useful to draft one set of maintenance of the law elements that would cover:[541]

- disclosing personal information to a law enforcement agency upon request;
- disclosing personal information to a law enforcement agency in the absence of a request;
- disclosing personal information by a law enforcement agency; and
- withholding personal information by a law enforcement agency.

The Department of Internal Affairs noted that it may be difficult to define which agencies are law enforcement agencies, as besides the core law enforcement agencies such as the Police and the Serious Fraud Office, a number of other public agencies have mixed functions that include enforcement as well as other functions.

537 Ibid, at [Q147].

538 Ibid, at [Q149].

539 Ibid, at [Q148].

540 Ibid, at [Q154].

541 Submission by the New Zealand Customs Service.

9.38 There was support from some submitters for greater clarity about information sharing between law enforcement agencies, although the Office of the Privacy Commissioner (OPC) reported that it is satisfied that the existing provision is adequate on this point.

9.39 A submitter from the private sector suggested that there should be a further exception to principle 11 to specifically allow for disclosure where a private sector agency reasonably suspects that unlawful activity has taken place or is likely to take place and that disclosure is necessary for the investigation of that activity by the agency. This suggestion is discussed in chapter 3.[542]

Reporting offending

9.40 The Police submitted to us that misunderstandings about the Privacy Act contribute to a reluctance amongst the public to report criminal offending and to share information with law enforcement agencies. Even where agencies do have a good understanding that the Privacy Act permits disclosure in appropriate circumstances, the Police believe that a risk-averse culture limits flows of information that would assist law enforcement agencies to carry out their functions effectively. At a forum organised by InternetNZ, it was noted that many people are apprehensive about breaching the Privacy Act if they report a possible crime, in both the online and the physical worlds.[543]

9.41 Proposed solutions that have been suggested to us include:

- People who provide information to law enforcement agencies in reliance on the maintenance of the law exception to principle 11 could be exempted from being subject to the Privacy Act complaints process, with the law enforcement agency to which disclosure is made being responsible under the complaints process instead.
- A provision similar to section 48 of the Official Information Act 1982 (OIA) could be enacted, which would exempt an agency from liability for any disclosure made in good faith in response to a request, in reliance on the maintenance of the law provision.

9.42 Another proposal was for an information campaign specifically about the reporting of crime under the Privacy Act.

A need for guidance

9.43 A number of submissions favoured information or guidance from the Privacy Commissioner about the maintenance of the law exception to principle 11. One agency suggested that this would improve understanding of and compliance with the Privacy Act.

9.44 Trade Me submitted that it would be useful from a practical perspective for agencies receiving requests for information from law enforcement agencies (without a warrant) to have guidance on what such requests should include, in order for the responding agency to be satisfied that there are reasonable grounds for requesting the information for law enforcement purposes. Trade Me

542 See [3.114]–[3.117].

543 InternetNZ Privacy Roundtables (Wellington, 21–22 June 2010).

suggested that guidance would help to ensure that requests from government agencies are properly authorised and tightly framed. The Police also submitted that it would be helpful to have more clarity around what constitutes a belief on "reasonable grounds" that a disclosure is necessary to avoid prejudice to the maintenance of the law.

Our response

A need for guidance

9.45 Although we suggested in the issues paper that the maintenance of the law provision be redrafted for greater clarity,[544] and asked if the maintenance of the law provision should be restructured,[545] we have concluded that much of the uncertainty and confusion about the provision could be addressed by guidance. We support the call in submissions for guidance from the Privacy Commissioner that explains how the maintenance of the law provision operates. This would assist to inform agencies of their rights and responsibilities in relation to the disclosure of personal information to law enforcement agencies.

9.46 We recommend that the Privacy Commissioner develop an information sheet or guidance on the maintenance of the law exception to privacy principle 11.[546] This should include guidance on responding to law enforcement requests for information and an explanation of the steps an agency should take to assure itself of the necessity for the disclosure. As part of this work, we recommend that the Privacy Commissioner consult with law enforcement agencies about the form and process for making requests for information under the Privacy Act. We consider guidance in this area to be a high priority for the Privacy Commissioner, based on the response in submissions, and the fundamental importance of the relationship between law enforcement objectives and privacy rights.

RECOMMENDATION

R96 The Privacy Commissioner should develop an information sheet or guidance on the maintenance of the law exception to principle 11. This should include guidance on responding to law enforcement requests for information and an explanation of the steps an agency should take to assure itself of the necessity for the disclosure. As part of this work, the Privacy Commissioner should consult with law enforcement agencies about the form and process for making requests for information under the Privacy Act.

544 Issues Paper at [Q147].

545 Ibid, at [Q148].

546 This should include guidance on principles 2, 3 and 10, to the extent that there any particular issues with the provision in those contexts.

Reporting of offending

9.47 We agree that the Privacy Act needs to clearly express that the public may cooperate with law enforcement agencies and report suspected offending without undue fear of privacy complaints being raised about the reporting.

9.48 We do not favour solutions proposed in submissions that would shift responsibility for disclosures from the disclosing agency to the agency receiving information or enact a liability exclusion provision similar to section 48 of the OIA. These solutions would be a significant departure from the framework of the Privacy Act which places accountability and responsibility on the disclosing agency. We also note that where law enforcement agencies meet with reluctance or resistance in responding to requests for information amongst members of the public or public or private sector agencies, there are a range of other tools that enforcement agencies can utilise in appropriate circumstances to compulsorily acquire information. We are not convinced that it is necessary to change the structure of the Privacy Act to deal with this concern.

9.49 Our preferred option is to create a further exception to principle 11 to specifically cover the reporting of offences. We therefore recommend a further exception that would expressly permit an agency to report any reasonably held suspicion or belief that an offence has been or may be committed, including any relevant information about that offence, to a public sector agency with law enforcement functions. This would provide an assurance to agencies (including members of the public) about their right to report suspected offending to the appropriate authorities. Any such disclosure would remain discretionary on the part of the disclosing agency or person, who would retain responsibility for the disclosure. Factors such as ethical responsibilities and obligations of confidence may weigh against an agency deciding to report suspected offending.

9.50 Another consideration is whether the creation of a specific exception to principle 11 covering the reporting of offending would encourage malicious reports to law enforcement or other public sector agencies. We think that such a provision would be appropriately balanced if reliance on it requires any suspicion about the offence being reported to be reasonably held by the person reporting it.

9.51 The amendment proposed to principle 11 would allow agencies (including members of the public) to volunteer personal information about others to enforcement agencies where there is a reasonably held suspicion or belief about criminal offending that requires investigation. Agencies and members of the public could also respond to requests for personal information about suspected offenders from the police and other enforcement agencies, either under the new exception proposed or under the maintenance of the law disclosure exception, depending on the circumstances. The agency or person to whom a request is directed would retain the discretion as to whether to disclose the requested information. To compel provision of the requested information would require the issue of a compulsory order such as a warrant or production order.

9.52 We do not propose that the class of public sector agency to which offending may be reported should be confined, given the wide range of public sector agencies that have enforcement functions. However, where offending is reported to one public sector agency but needs to be investigated or prosecuted by another agency, a further disclosure of the information will be required by to the appropriate agency. Generally, such further disclosures by an intermediary agency would fall within the maintenance of the law exception to principle 11.

9.53 We support the proposal in submissions for an information campaign about the reporting of crime under the Privacy Act, and recommend that the Privacy Commissioner and the Police consider working collaboratively on such an initiative. We note that both the Police and the Privacy Commissioner are partner agencies of NetSafe in its launch of "the orb". "The orb" is an online crime reporting mechanism that has been developed to offer a simple and secure way to report online incidents that may break New Zealand law, such as objectionable material that may breach censorship laws, child pornography and offending against children, scams and frauds, spam, computer system attacks, breaches of the consumer legislation by online traders and privacy breaches.[547] An information campaign about the reporting of crime would assist to publicise this initiative, as well as the proposed clarification in the Privacy Act to provide greater assurance to the public that the Privacy Act is not a barrier to the reporting of suspected offending to the appropriate agencies.

RECOMMENDATION

R97 A new exception to principle 11 should be created that would expressly permit an agency to report any reasonably held suspicion or belief that an offence has been or may be committed, including any relevant information about that offence, to a public sector agency with law enforcement functions.

RECOMMENDATION

R98 The Privacy Commissioner and the Police should consider working collaboratively on an information campaign about the reporting of crime under the Privacy Act.

547 < www.theorb.org.nz > .

Part 11 and Schedule 5

9.54 Part 11 of the Privacy Act establishes a framework for the sharing of law enforcement information about particular individuals between public sector agencies. Schedule 5 to the Privacy Act contains the list of authorised arrangements for the sharing of particular law enforcement information between agencies such as the Police, Ministry of Justice, Department of Corrections, and the New Zealand Transport Agency. In the issues paper we asked four questions about Schedule 5 to the Privacy Act:

- Should the sharing of law enforcement information continue to be dealt with under a specific schedule to the Privacy Act, or should this be dealt with in regulations or a code of practice?[548]
- Should additional transparency measures (such as those that apply to information matching) apply to law enforcement information sharing, or could this information sharing be dealt with under a generic information sharing mechanism?[549]
- Should Schedule 5 continue to provide for local authorities to access law enforcement information?[550]
- Should the power to amend Schedule 5 by Order in Council be reinstated and, if so, should the power be subject to a sunset clause?[551] What safeguards would be needed?[552]

Submissions

9.55 Few submissions addressed the questions asked about Schedule 5. The submissions that did comment on these questions showed support for retaining the law enforcement information sharing mechanism, although submitters were generally open to altering the legislative vehicle to either regulations or a code of practice. There was support for additional transparency measures, although two agencies opposed these.

9.56 In submissions responding to the question of whether provision for local authority access to these registers under Schedule 5 should be maintained, while the New Zealand Transport Agency stressed that access is critical for enforcement purposes, OPC noted a finding from an earlier review that local authorities use other statutory authority to gain access to the registers. The Police suggested that it would be more appropriate to deal with local authority access to these registers through other statutory authority.

9.57 There was support for reinstating the power to amend Schedule 5 by Order in Council, although two agencies opposed this. However, it was noted that if the content of Schedule 5 was shifted to regulations, this issue would not arise. If the power was to be reinstated, suggestions for safeguards included a

548 Issues Paper at [Q150].

549 Ibid, at [Q151].

550 Ibid, at [Q152].

551 Upon enactment, the Privacy Act contained a power to amend Schedule 5 by Order in Council (s 113); however this power expired on 1 July 1997 due to a sunset provision (s 114) and has never been reinstated. This has meant that any change to Schedule 5 has had to be effected through legislative amendment.

552 Issues Paper at [Q153].

requirement to consult OPC, a requirement to submit a Privacy Impact Assessment to the Cabinet (in the same way that a Bill of Rights Act vet is required) and submitting to the Regulations (Disallowance) Act 1989.

Our response

New information sharing framework

9.58 Following release of the issues paper, the Law Commission conducted further work in the area of government information sharing, which has proved to be a major development during the course of the review. In the Ministerial Briefing issued in advance of this report, the Law Commission proposed a new framework for the Privacy Act to cover government information sharing and matching under authorised programmes.[553]

9.59 In developing the proposed new framework, we considered whether Schedule 5 should continue to exist in some form as a separate framework. However, we have concluded that a separate regime for law enforcement information sharing is not necessary and that the law enforcement information sharing currently authorised by Part 11 and Schedule 5 should become part of the proposed new information sharing framework, although existing arrangements in Schedule 5 would be grandparented.[554] This would effectively replace Schedule 5 with equivalent regulations, while the Schedule 5 particulars would be listed in a new schedule to the Privacy Act as part of the proposed list of authorised information sharing programmes.[555]

9.60 We therefore recommend that Part 11 of the Privacy Act should be repealed, subject to transitional provisions to grandparent law enforcement information sharing as contained in Schedule 5. New law enforcement information sharing initiatives should be subject to the rules of the new information sharing framework. We believe that this change would create greater simplicity, clarity and consistency, as well as improved checks, balances and safeguards for information sharing.

9.61 Rolling Schedule 5 into the new information sharing framework would also deal with some of the issues we asked about in the issues paper. One of those issues is the need for flexibility to amend the parameters of particular law enforcement information sharing programmes without calling on the considerable resources involved in pursuing parliamentary enactment, while ensuring that suitable safeguards apply. Under the proposed information sharing framework, it is envisaged that new information sharing programmes would be created or amended by Order in Council, subject to disallowance under the Regulations (Disallowance) Act 1989. It is also proposed that OPC could initiate a review of any particular information sharing programme.

9.62 Secondly, we asked about improved transparency measures. The new information sharing framework specifically addresses transparency. It would require publication of the text of the applicable protocol or information sharing agreement,

553 Appendix 1.

554 Appendix 1, at [62]–[64], proposal (5).

555 Ibid, proposal (8).

regular reporting on the operation of the information sharing programme by the agency concerned, and inclusion of the information sharing programme in a statutory list.

9.63 Thirdly, on the issue of local authority access to law enforcement information, this access under Schedule 5 is limited to the driver licence and motor vehicle registers, where authorised by the Minister by notice in the Gazette,[556] or under any surviving notice given under section 4E of the Wanganui Computer Centre Act 1976.[557] We do not believe that it is necessary to continue to provide access to the driver licence and motor vehicle registers by this mechanism. Access to public registers for law enforcement purposes should be authorised through the relevant statutory provisions establishing these registers.[558] The Land Transport Act 1998 has been amended to specifically state the purposes of the motor vehicle register which include enforcement of the law.[559] There is also a process for the Secretary to approve access to name and address information (after consultation with the Privacy Commissioner, the Chief Ombudsman and the Commissioner of Police) for certain purposes.[560] We recommend that this new mechanism in the Land Transport Act be used to provide for access to the driver licence and motor vehicle registers, in place of the Schedule 5 mechanism.

RECOMMENDATION

R99 Further to proposal 5 in Appendix 1, Part 11 of the Privacy Act should be repealed, subject to transitional provisions to grandparent law enforcement information sharing arrangements that are currently contained in Schedule 5.

RECOMMENDATION

R100 Access to public registers such as the driver licence and motor vehicle registers should be dealt with under the relevant statute authorising the particular register.

556 Privacy Act 1993, s 112(1).

557 Privacy Act 1993, s 112(4). The relevant notice was published in the *Gazette* on 2 August 1990 and authorises Dunedin, Lower Hutt and Tauranga City Councils to access these registers only for the purposes of enforcing parking by-laws. Subsequent notices authorise access by Wellington, Auckland and Manukau City Councils for the same purpose.

558 See also the recommendations in Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, 2008).

559 Land Transport Act 1998, s 235.

560 Land Transport Act 1998, s 241.

Chapter 10
Technology

10.1 The technological landscape in which the Privacy Act operates today is very different to the landscape in which the Privacy Act was passed in 1993. While computer technology and the internet had arrived by 1993 and presented challenges to traditional paper-based methods of information handling, those developments have now assumed a central place both in the economy and in people's lives. They have also continued to raise significant implications for the handling of people's personal information.[561]

10.2 Advances in information, communication and surveillance technologies have created and intensified a range of privacy issues.[562] The Privacy Commissioner has described it as a "technology tidal wave," the effects of which are yet to clearly emerge.[563] Key aspects of information handling with which the Privacy Act is vitally concerned, namely the collection, use and disclosure of personal information, have been transformed. Notable changes have been the ease with which personal information is distributed around the globe, the pervasiveness and longevity of personal data, and the creation of commercial opportunities and incentives to commoditise personal information due to the increasing economic value of consumer data.

OUR EXAMINATION OF THE ISSUES

10.3 In the issues paper we dedicated a chapter to the interface between the Privacy Act and specific technological developments,[564] such as the internet (including issues raised by search engines, websites and social networking), cloud computing,[565] deep packet inspection,[566] location technologies,[567] radio

561 See generally Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008) at ch 6 [*Privacy: Concepts and Issues*].

562 See Office of the Privacy Commissioner (Australia) "New Privacy Commissioner Ready to Respond to Privacy Challenges" (media release, 22 July 2010) < www.privacy.gov.au > .

563 Office of the Privacy Commissioner *Statement of Intent 2010–2013* (2010) at 3 [*Statement of Intent*].

564 Issues Paper at ch 13. See also Law Commission *Privacy: Concepts and Issues*, above n 561, at ch 6.

565 Cloud computing describes the trend towards accessing computer processing and data storage facilities from service providers on the internet, instead of using packaged software and dedicated hard drives or network servers. See Australian Government, Department of Defence, Intelligence and Security Cyber Security Operations Centre Initial Guidance "Cloud Computing Security Considerations" (12 April 2011) < www.dsd.gov.au > .

566 Deep packet inspection is a form of computer network packet filtering (including packet content) that can be used for a range of services including the management of network performance and security by internet service providers.

567 Location technologies provide services based on a person's location, through the use of location data.

frequency identification[568] and biometrics.[569] The interface between technology and privacy was also a constant theme throughout the paper, for example in chapters relating to the Privacy Act definitions,[570] information matching,[571] information sharing,[572] trans-border data flows[573] and direct marketing.[574] We also asked whether any particular protections for young people are required in relation to online privacy.[575]

10.4 In this final report, we have also considered technological issues throughout and we have recommended changes where we think the Privacy Act requires adaptation to meet challenges to the protection of personal information.[576] The Act must be effective so far as possible in both the online and offline aspects of people's lives.

10.5 In this chapter we consider the issues raised by technology from a generic perspective. We discuss whether any changes to the Privacy Act are needed to respond to the exponential rate of technological change since the Act was passed, or to respond to any particular practice that has arisen through technological development. Related to this, in the following chapter we recommend changes to the Privacy Act to protect personal information that is transferred out of New Zealand by agencies that have collected it, for example, via cloud computing.[577]

10.6 Apart from the specific changes we outline elsewhere in the report, we are not persuaded that many changes are needed to the Privacy Act itself. On the whole, we think that the privacy principles and the Privacy Commissioner's current functions and powers are adequate and sufficiently flexible to respond to the challenges posed by new technologies. Nevertheless, that landscape is dynamic and will need to be kept under regular review to ensure that this remains the case. The most significant change we propose in this chapter is that clear expectations as to the use of privacy impact assessments in the public sector should be articulated in a Cabinet Office circular and State Services Commission guidance.

568 Radio frequency identification or RFID is a tagging technology developed for inventory control that can be used to track items or people in a range of contexts.

569 Biometric technologies use biological characteristics to identify individuals (such as finger and iris scanning, and facial, voice and gait recognition).

570 Issues Paper at ch 3.

571 Ibid, at ch 9.

572 Ibid, at ch 10.

573 Ibid, at ch 14.

574 Ibid, at ch 15, [Q169].

575 Ibid, at ch 18, [Q187].

576 See R7 (clarify the definition of "collect"); R8, R10 (reform the definition of "publicly available publication"); R35 (option of anonymity); R43–R45 (changes to s 56); R64 (Privacy Commissioner audit power); R67–R69 (data breach notification requirement); R107–R115 (overseas transfers of personal information); R117–R118 (unique identifiers and identity crime); R120–R122 (young people online); R127–R136 (information matching).

577 Ch 11 at R107– R115. See also [10.84]–[10.89].

10.7 We also discuss in this chapter ways in which current provisions of the Privacy Act, including the Privacy Commissioner's existing functions and powers, might be used to respond to current privacy challenges. In particular, we consider the function of undertaking educational programmes to promote the protection of privacy[578] to be key.

PRIVACY COMMISSIONER'S FUNCTIONS

10.8 The Office of the Privacy Commissioner (OPC) has said that:[579]

> We act as a watchdog of big and small information systems and provide targeted assistance and advice. The invasion of technology into almost every aspect of day to day life accentuates the need to help both organisations and individuals handle personal information well. We raise awareness of information risks and benefits, and provide self help tools.

10.9 In the technology chapter of the issues paper, we asked whether any changes to the Privacy Commissioner's functions are required.[580] We noted that certain functions of the Privacy Commissioner specifically relate to technological developments.[581]

Submissions

10.10 A number of submitters were comfortable with the Privacy Commissioner's current functions with respect to technology issues. Others put forward various suggestions such as:

- the Privacy Commissioner should have a broad technology related function along the lines of "how to manage the privacy principles with regard to technology impact and changes";
- the Privacy Commissioner's educative function in relation to technology should be expanded and enhanced;
- the Privacy Commissioner's role should include the development of guidelines;[582]
- a code of practice or guidelines relating to technology would be appropriate;[583]
- the Privacy Commissioner's staff should include a qualified adviser on digital and online communication technologies; and
- the Privacy Commissioner should have a specific role in relation to cloud computing.

578 Privacy Act 1993, s 13(1)(g).

579 Office of the Privacy Commissioner *Statement of Intent*, above n 563, at 3.

580 Issues Paper at [Q155].

581 Ibid, at [13.9]; Privacy Act 1993, s 13(1)(m) and (n).

582 This submission noted that this role would need to be adequately resourced.

583 In its submission, Google expressed the view that the Privacy Commissioner should only issue guidance after consultation with affected stakeholders and other interested parties.

10.11 OPC's submission noted that any reformulation of the Privacy Commissioner's functions must be expressed in sufficiently general and flexible terms to remain useful for the next 20 years. The Privacy Commissioner's view is that her functions in section 13(1)(m) and (n) remain sufficiently generic to work as well in the present day as in 1993, although the word "computer" could be dropped from section 13(1)(n) now that computers are so common as not to need to be particularly identified and to avoid any potential exclusion of other technologies.

Our response

10.12 We agree that the current formulation of the Privacy Commissioner's functions (both the functions that specifically refer to technology as well as the Commissioner's general functions relating to education, guidance, advice, public statements, research and monitoring, inquiries, reporting to government and cooperation with international bodies) are generally flexible enough to allow the Privacy Commissioner to address privacy issues associated with technology that affect New Zealanders.[584] On the whole, we think that the Privacy Act already allows the Privacy Commissioner to respond to technologies in the ways suggested in submissions, such as producing guidelines or coordinating a particular code of practice as appropriate, undertaking additional educational measures, and focusing on particular developments such as cloud computing. The key limitations to undertaking any such initiatives are limits on funding and resources. This means that the Privacy Commissioner must carefully prioritise the work undertaken by the Office.

10.13 We agree with the Privacy Commissioner's suggestion that her technology function in section 13(1)(n) should be broadened by deleting the word "computer". The Australian Law Reform Commission made a similar recommendation in relation to the Australian Privacy Act, which has been accepted by the Australian Government.[585]

10.14 We consider the Commissioner's function to undertake educational programmes to promote the protection of privacy to be a key one in responding to privacy challenges arising from technological developments. This is of particular importance during the bedding-in stage of a technology where there may be a lack of awareness or uncertainty as to the privacy implications.

10.15 There are two aspects to the educational function:

- assisting agencies to interpret and apply the privacy principles in new technological contexts,[586] and
- assisting individuals to engage with new technologies in a privacy-protective manner.[587]

---

584 See for example the Privacy Commissioner's investigation into Google's collection of WiFi data during StreetView filming: Office of the Privacy Commissioner "Google Agrees to Protect Privacy Better" (media release, 14 December 2010); "Google WiFi Investigation" *Private Word* (December 2010).

585 *For Your Information*, R47–1; *Enhancing National Privacy Protection* at 85.

586 The Privacy Commissioner has noted increasing demand from agencies for information and guidance from the Privacy Commissioner: Office of the Privacy Commissioner *Statement of Intent*, above n 563, at 6.

587 The Privacy Commissioner has noted a lack of individual awareness about "safe" practice, especially online: ibid, at 6.

Both aspects are important to ensure that the privacy of New Zealanders continues to be adequately protected during periods of technological change.

10.16 A different form of education is the Privacy Commissioner's function to monitor technological developments that may impact on privacy and to report on these developments to government or to the wider public.[588] The fulfilment of this function is critical to ensure that policymakers have access to quality information about the potential impacts that use of a technology may give rise to. It also provides an opportunity for the Privacy Commissioner to inform and raise awareness (especially within the public sector) as an initial step in encouraging Privacy by Design, a concept that is discussed later in this chapter. The Privacy Commissioner fulfils this function in a number of ways including the technology section of OPC's website; by including a brief report on technology policy in the Office's Annual Report; by signalling technology issues and their impact on the work of the Office in the Statement of Intent; by including items on technological issues in the bulletin *Private Word*; by making submissions on legislation that mandates the use of particular technologies; and by reporting on specific projects undertaken by the Office such as the CCTV guidance[589] and the survey on portable storage devices.[590]

10.17 We have also recommended in an earlier report that the Privacy Act should provide that one of the functions of the Privacy Commissioner is to report regularly to Parliament on developments in surveillance and surveillance technologies, and their implications for New Zealand.[591]

10.18 We think it is valuable for the Privacy Commissioner to continue to provide information highlighting new technologies that may raise potential privacy issues. To raise awareness of cutting edge technologies and their potential privacy implications, consideration could be given to making more information available at an earlier stage, that is to say, at a stage where OPC is aware of potential privacy issues pertaining to a technology but where the Office has not necessarily formed a definitive view or any official guidance about these issues. Providing information as it comes to hand would serve as a first step in signalling to agencies that privacy will need to be taken into account in conjunction with the utilisation of these technologies. We think that there is further scope for the Privacy Commissioner to provide occasional bulletins and updates on new technologies. Such updates could discuss overseas approaches, developments and experiences from a privacy perspective, as well as New Zealand initiatives and perspectives.[592]

588 Privacy Act 1993, s 13(1)(n), s 13(1)(h).

589 Office of the Privacy Commissioner *Privacy and CCTV: a Guide to the Privacy Act for Businesses, Agencies and Organisations* (2009).

590 Office of the Privacy Commissioner *Guidance Note on Portable Storage Devices* (2009).

591 Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, 2010) at R18 [*Penalties and Remedies*].

592 See for example the Victorian eGovernment Resource Centre "Privacy – Topics A-Z" < www.egov.vic.gov.au > .

10.19 We think that this would assist to raise awareness of current and potential privacy issues, contribute to informing public debate, entrench the role of the Privacy Commissioner as a public advocate for privacy issues as new privacy challenges arise and encourage consultation with the Office by agencies investigating the adoption of these technologies (thus contributing to better privacy outcomes). The Office should be well placed to comment on technological developments and their potential implications, given the Privacy Commissioner's active participation in international privacy forums that provide dialogue and debate on cutting edge issues.[593]

10.20 One of the commendable initiatives of the Office is the occasional Privacy and Technology forums which are often oversubscribed. We suggest that these valuable sessions could have wider reach if the content is more consistently made available through the internet, whether in video, podcast or transcript form.

10.21 We acknowledge that any additional work undertaken in this area would be subject to resourcing and prioritisation of the Office's workload. As the Privacy Commissioner has noted, the Office is a small organisation and must make intelligent choices and work in partnership with others.[594] Later in this chapter we suggest that the Privacy Commissioner consider establishing an expert committee on Privacy by Design. One task of this Committee could be to recommend items for inclusion in the Office's work plan, as resources and other priorities permit.

10.22 On the question of technical expertise within the Privacy Commissioner's Office, we note that the Office recruits staff with technological expertise to its technology team, as resources permit.[595] Technology and privacy is an area where it is important for the Privacy Commissioner to coordinate with other organisations to harness appropriate expertise and we note, for example, the relationship between OPC and NetSafe in promoting awareness of online safety. Another partnership opportunity may be to seek to strengthen the relationship between OPC and InternetNZ. Expertise could also be maximised through the use of expert panels, which we now address.

RECOMMENDATION

R101 Section 13(1)(n) should be amended to delete the word "computer."

593 For example, the Asia Pacific Privacy Authorities (APPA) forum has established a working group on technology issues: Office of the Privacy Commissioner "Privacy Commissioners Commit to Continue International Collaboration" (media release, 9 December 2010).

594 Office of the Privacy Commissioner *Statement of Intent*, above n 563, at 3.

595 In the Issues Paper at [13.11]–[13.15] we noted the work of the Office of the Privacy Commissioner in relation to technology issues.

ADVISORY AND EXPERT PANELS

10.23 In the issues paper, we asked whether the Privacy Act should expressly provide for a Privacy Advisory Panel or for the Privacy Commissioner to be able to convene expert panels on certain topics.[596] We noted that the Australian Privacy Act expressly provides for a government-appointed Privacy Advisory Committee that includes a person experienced in information and communication technologies. The Australian Government has also accepted the recommendation of the Australian Law Reform Commission (ALRC) that the Australian Privacy Act should expressly empower the Australian Privacy Commissioner to establish expert panels.[597] These are panels that can be convened at the Privacy Commissioner's discretion. In the United Kingdom, the Information Commissioner's Office is in the process of establishing a technology reference panel of industry experts.[598]

Submissions

10.24 A number of submitters agreed that the New Zealand Privacy Act should provide for advisory or expert panels; however some submitters, including OPC, thought that expert panels can be established under current powers, and that no statutory amendment is required. The Privacy Commissioner noted that external reference groups of experts have been convened from time to time, such as for the review of the Credit Reporting Code, as well as the Youth Advisory Group.

Our response

10.25 We agree with the view that current powers are sufficient for the Privacy Commissioner to establish expert panels on particular topics. Later in this chapter we recommend that the Privacy Commissioner consider establishing a Privacy by Design Committee. We also suggest that consideration could be given to establishing an expert committee on cloud computing, or alternatively, cloud computing could be one of the issues addressed by a Privacy by Design Committee.

10.26 We do not recommend the creation of a Privacy Advisory Committee by government appointment. In order for the Privacy Commissioner to make most efficient use of scarce resources, we think that it would be preferable for the Commissioner to establish expert committees on particular issues as priorities demand and as resources allow. We do not believe that a permanent advisory committee would necessarily offer best value for the significant cost that establishing such a body may involve.

596 Ibid, at [Q156].

597 *For Your Information* at R46–5; *Enhancing National Privacy Protection* at 84.

598 Information Commissioner's Office (UK) *Upholding Information Rights: ICO Corporate Plan for 2011–2014* (2011).

APPROACH OF THE PRIVACY ACT TO TECHNOLOGY

10.27 In the issues paper we asked whether the basic framework of the Privacy Act with its technology-neutral privacy principles is adequate to deal with the challenges of technological change.[599]

Submissions

10.28 The overwhelming majority of submitters responding to this question agreed that technology-neutral privacy principles should be retained. Some submitters noted and approved of the use of Codes of Practice to modify the application of the privacy principles in particular circumstances.

10.29 Some submitters noted that technology can raise particular issues as to the operation of the privacy principles. The Health Research Council noted that key privacy principle concepts such as notice and consent may not always be effective in the online environment and that consumers do not always know what they are consenting to, especially with regard to secondary uses of their data and who it will be shared with. Legal academic Gehan Gunasekara noted some uncertainty about whether the Act is adequate to deal with future developments, suggesting that possible solutions might include greater openness and transparency, the monitoring of technology uses and the use of expert panels to advise the Privacy Commissioner. OPC noted the role of international cooperation in identifying global responses to technology-related privacy issues.

Our response

10.30 We are satisfied that overall, the current approach of using technology-neutral privacy principles in the Privacy Act should be retained. The OECD has concluded that technology neutral principles have been a "remarkable success"[600] and the approach is consistent with that taken in other jurisdictions such as Australia,[601] the European Union[602] and Canada.[603] In the United States, policymakers have recommended consideration of comprehensive fair information practice principles to close gaps in current sectoral privacy laws and to provide more uniform commercial privacy protection across industries and data uses.

599 Issues Paper at [Q157].

600 Organisation for Economic Co-operation and Development *The Evolving Privacy Landscape: 30 Years After the OECD Guidelines* (DSTI/ICCP/REG(2010)6/REV2) at 4–6.

601 See Australian Law Reform Commission "Technology-neutral Privacy Principles Should Govern Rapidly Developing ICT" (media release, 11 August 2008); *For Your Information* at [10.9]–[10.12]; Office of the Privacy Commissioner (Australia) "The Adequacy of Protections for the Privacy of Australians Online" (Submission to the Senate Standing Committee on Environment, Communication and the Arts, August 2010).

602 See Article 29 Data Protection Working Party *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the Fundamental Right to the Protection of Personal Data* (1 December 2009, 02356/09/EN WP 168) which finds the main principles of data protection still valid despite new technologies and globalisation.

603 See Office of the Privacy Commissioner (Canada) *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing* (May 2011) at 7, 22 [*Consultations Report*], noting that the Personal Information Protection and Electronic Documents Act (PIPEDA) has been able to adapt to technologies and business models that did not exist when it first came into force.

10.31 Nevertheless we note that technology issues will continue to raise privacy challenges. From submissions to the issues paper and from our research we note that questions are being asked about the adequacy of privacy frameworks to fully address privacy issues raised by developments in technology and new applications.[604] It will therefore be important that subsequent reviews of the Privacy Act ensure that the Act continues to adequately deal with technology issues and to reflect international responses to those issues that may be developed in the future through global cooperation and consensus.

10.32 One area that we think will need to be kept under review is the threshold definition of "personal information."[605] Currently, only information that is about an identifiable individual is covered by the privacy principles. A growing category of information for which people may expect privacy protection is information such as search history and location data that can be linked to a particular computer or device by virtue of an Internet Protocol (IP) address or unique device identifier (UDID).[606] Advances in analytics and the decreasing effectiveness of anonymisation mean that more data can potentially be linked to an individual and aggregated with other data relating to that individual. However, the boundaries between personal information and non-personal information are currently somewhat opaque and whether information that can be linked to a personal device may considered to be "personal information" depends on the circumstances. The clarity and scope of the definition of "personal information" may therefore need to be addressed in future reviews of the privacy framework.[607]

10.33 Another key concept is "publicly available information." Generally information that is "publicly available" falls outside the scope of the privacy principles. The rise of social networks in particular has blurred the line between private and publicly available information. While we have recommended amendments to the Privacy Act definition and scope of "publicly available publication"[608] and that the Privacy Commissioner should produce guidance,[609] this is another area that may need to be kept under review.

10.34 Another fundamental aspect of the privacy principles is the notice principle and its relationship with consent.[610] In the online context, there are issues with lengthy privacy notices failing to efficiently inform consumers about their

604 See for example Judge David Harvey "Privacy and New Technologies" in Steven Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (Brookers, Wellington, 2010) at 330–333, 346–347.

605 See also [2.38]–[2.53].

606 See United States Federal Trade Commission *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (preliminary FTC staff report, December 2010) at 43, seeking feedback on a proposed framework that would apply to both personally identifiable information and data that can be reasonably linked to a specific computer or other device.

607 For discussion of some issues about personal information, see ibid, at 35–38; Office of the Privacy Commissioner of Canada, *Consultations Report*, above n 603, at 23–24; William B Baker and Anthony Matyjaszewski "The Changing Meaning of Personal Data" International Association of Privacy Professionals < www.privacyassociation.org > .

608 See R8, R10.

609 See R9.

610 For discussion of this issue see Office of the Privacy Commissioner of Canada *Consultations Report*, above n 603, at 24 –28; Parliament of Australia, Environment and Communications References Senate Committee *The Adequacy of Protections for the Privacy of Australians Online* (7 April 2011) at [3.15]–[3.31].

privacy options. This is an area where technological options may in future assist consumers to manage their privacy, in addition to regulatory or legislative solutions. Privacy notices are discussed further below.

RECOMMENDATION

R102 The technology-neutral privacy principles should be retained. However, during this period of rapid technological change, the principles should be regularly reviewed (5-yearly) to ensure that the Privacy Act continues to effectively respond to privacy issues raised by technological developments.

PRIVACY-ENHANCING TECHNOLOGIES AND PRIVACY BY DESIGN

10.35 According to the Office of the Australian Privacy Commissioner:[611]

> Digital technologies can be configured to allow individuals to remain anonymous or use a pseudonym, to limit the amount of personal information collected, to obtain and manage consent, to limit the scope for unintended secondary uses of personal information, to provide individuals with greater choice in relation to their personal information, to detect privacy settings and so on. These are commonly referred to as privacy enhancing technologies (PETs).

10.36 Privacy by Design is a term used to describe the proactive process of incorporating PETs where appropriate into new information systems and information handling processes.[612] In the technology chapter of the issues paper we asked whether express provision should be made in the Privacy Act for privacy-enhancing technologies.[613]

Submissions

10.37 There was a range of opinion in submissions about the role of the Privacy Commissioner in relation to privacy-enhancing technologies (PETs) and whether the Privacy Act should include any legislative compulsion to use PETs. InternetNZ noted that insufficient attention has been given to developing and implementing PETs in New Zealand. One public sector agency suggested that the use of PETs could be mandated by regulation or legislation, while a private sector submitter did not see the Privacy Commissioner as having any role in the approval of the design of technological tools. Other submitters thought that the role of the Privacy Commissioner here should be primarily educative, both in terms of educating agencies about best practice measures such as encryption, and in terms of educating citizens about what steps they can take to protect their privacy when using a technology.

10.38 The Privacy Commissioner submitted that OPC might have a useful role in educating industry and the public about the available technologies and about the ways in which they can protect individuals or assist in privacy compliance.

611 Office of the Privacy Commissioner (Australia), above n 601, at 18.

612 See Information and Privacy Commissioner of Ontario "Privacy by Design: the Seven Foundational Principles" < www.privacybydesign.ca > .

613 Issues Paper at [Q158]. See also Law Commission *Privacy: Concepts and Issues*, above n 561, at [6.106]–[6.113].

The Privacy Commissioner noted that OPC might also have a role in researching or encouraging research in relation to PETs, although the Office would need to be resourced to commission research in this area.[614]

Our response

10.39 We think that PETs have an important role to play in ensuring that the standards embodied in the privacy principles are observed in a wide range of personal information handling contexts. However, we think that it would run counter to the flexibility of the privacy principles and their technological neutrality for the Act to specify that any particular measures must be taken. It may also be counterproductive to mandate that certain PETs must be used, given the rapid rate of technological development. Nevertheless, it may be appropriate for a Code of Practice to spell out particular measures or standards that should be adopted in a particular context.

10.40 Our preferred approach is for the Privacy Commissioner, through the Commissioner's existing functions,[615] to continue to highlight the role of PETs and raise awareness of how and when such technologies can be adopted by agencies in personal information handling.[616] The Commissioner should also highlight steps that consumers can take to control and protect their personal information. This will involve the development of materials by OPC to inform New Zealanders, but OPC may also be able to draw on materials produced by other Privacy Commissioners and Data Protection Commissioners as well as other bodies through links on OPC's website.[617]

10.41 This is consistent with the approach taken by the ALRC, an approach that has been accepted by the Australian government. The ALRC recommended that in exercising its research and monitoring functions, the Office of the Australian Privacy Commissioner should consider technologies that can be deployed in a privacy-enhancing way by individuals, agencies and organisations;[618] and should develop and publish educational materials for individuals and agencies about specific PETs and the privacy-enhancing ways in which technologies can be deployed.[619]

---

614 For example the Office of the Privacy Commissioner (Canada) allocates funding each year for non-profit research into privacy, including research into privacy information technology: "Canada's Privacy Commissioner Awards $454,000 for Privacy Research and Awareness" (press release, 29 May 2009).

615 See for example, the functions of the Privacy Commissioner under s 13(1)(g) (to undertake educational programmes), s 13(1)(h) (to make public statements), s 13(1)(i) (to receive and invite representations from the public), s 13(1)(j) (to cooperate with other persons and bodies concerned with privacy), s 13(1)(k) (to make suggestions on the need for any action in the interests of privacy), s 13(1)(m) (to inquire into any practice, procedure or technological development if privacy may be being infringed), s 13(1)(n) (to undertake research and monitor developments in technology), s 13(1)(q) (to report to the Prime Minister on the need to take any action to protect privacy), and ancillary functions in s 13(1)(s) and (t).

616 See for example the Information Commissioner's Office (UK) *Privacy Enhancing Technologies (PETs)* (Data Protection Note, 29 March 2007).

617 For example, see the privacy tools discussed in the report of the Federal Trade Commission, above n 606, at 28. See also the 2011 Develop for Privacy Challenge < www.develop4privacy.org > .

618 *For Your Information* at R10–1; *Enhancing National Privacy Protection* at 30.

619 *For Your Information* at R10–2; *Enhancing National Privacy Protection* at 30. See also Office of the Privacy Commissioner (Australia), above n 601, recommending the development and greater use of PETs to promote greater awareness.

10.42 From consultation we note that OPC is keenly aware of the potential of PETs to assure privacy protection and we are confident that the Privacy Commissioner will promote awareness of PETs as priorities and resources permit.[620] The Privacy Commissioner has also demonstrated a commitment to the principles of Privacy by Design in co-sponsoring a resolution that was passed at the 2010 International Conference of Data Protection and Privacy Commissioners recognising the concept of privacy by design as an essential component of fundamental privacy protection and encouraging Data Protection and Privacy Commissioners to promote privacy by design, foster the incorporation of its principles into privacy policy and legislation in their respective jurisdictions and encourage research into privacy by design.[621]

10.43 While we do not make any specific recommendations in relation to privacy-enhancing technologies in this report, we do recommend that the Privacy Commissioner consider convening an expert privacy by design panel. We suggest that this expert panel meet periodically to advance the promotion of the principles of privacy by design. As part of this, the panel could pool knowledge and expertise about PETs. The panel could issue a general invitation to agencies who may wish to consult it from time to time for advice on projects that raise privacy design issues.[622] The Privacy Commissioner could recommend that public sector agencies consult this panel in relation to projects that the Privacy Commissioner considers may raise important privacy issues.

10.44 A Privacy by Design Panel could help raise awareness of PETs, promote best practice and promote privacy by design, especially within the public sector.[623] By bringing together experts from both the public sector (such as OPC, the State Services Commission and the Department of Internal Affairs) and the private sector, a panel may be an efficient way to promote PETs without placing an additional resource burden solely on OPC. A multi-disciplinary panel may also facilitate linkages between OPC and government departments that may prove useful as the era of technological transformation continues. One potential linkage for the panel would be liaison with the Government ICT Council, the cross-agency initiative to transform government ICT solutions and implement the Directions and Priorities for Government ICT policy framework.[624]

10.45 We note research undertaken in the United Kingdom that identifies market imperfections such as asymmetric information, externalities, lack of information sharing about privacy risks and coordination failures leading to underinvestment in PETs. The research supports a potential public sector role to ensure that sufficient PET development is taking place and to help agencies overcome

620 For example, OPC contributed to New Zealand Computer Society *Professional Knowledge Curriculum* (September 2009) in relation to managing personal information, including privacy by design.

621 Information and Privacy Commissioner (Ontario) "Landmark Resolution Passed to Preserve the Future of Privacy" (press release, 29 October 2010).

622 See for example the model of the Legislation Design Committee that by invitation advises government departments in relation to the principles of legislative design.

623 See Law Commission *Privacy: Concepts and Issues*, above n 561, at [6.113], noting the potential roles for government policy in promoting PETs.

624 Department of Internal Affairs "Government ICT Council established" (media release, 22 December 2010).

barriers to deploying PETs.[625] The study also suggests that governments have a fundamental role in formulating standards of privacy protection and that public sector endorsements and official certification schemes can help raise awareness of PETs and increase consumer trust (yielding economic benefits).[626] We think that these issues should be investigated and progressed by the proposed Privacy by Design Panel.

RECOMMENDATION

R103 The Privacy Commissioner should consider convening an expert Privacy by Design Panel to promote privacy by design and to raise awareness of privacy-enhancing technologies.

PRIVACY IMPACT ASSESSMENTS

10.46 A privacy impact assessment (PIA) is a planning tool that agencies can use to assess the likely and possible impacts a project may have on privacy and to explore options to mitigate those privacy risks. The PIA is not limited to consideration of technology issues but is a useful way to assess the impact of a new technology on privacy. A PIA may be used at several stages in the life of a project. Currently the Privacy Commissioner encourages agencies to use this tool and has issued guidance in the form of a Privacy Impact Assessment Handbook.[627] In some cases, there is a legislative requirement to carry out a PIA.[628]

10.47 In the context of government information sharing, we recommend in appendix 1 that information sharing agreements would have to contain PIA-type matters such as a clear statement of the uses to which a recipient agency may put the information, a description of the safeguards to be adopted to ensure the security of the information shared and details of how general requirements of the Privacy Act relating to sharing programmes are to be met.[629] We also note that OPC might require a PIA to be undertaken in the case of more extensive programmes.[630]

10.48 In the issues paper we asked whether consideration should be given to empowering the Privacy Commissioner to direct public or private sector agencies to produce a PIA for projects that may significantly impact on the handling of personal information.[631]

625 London Economics *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs): Final Report to the European Commission* (July 2010).

626 See Lin Shu-yuan and Christie Chen "Taiwan to Issue Data Protection Privacy Mark" Focus Taiwan (8 April 2011) < http://focustaiwan.tw > reporting that the Taiwan Ministry of Economic Affairs is to issue data privacy protection marks (modelled on Japanese and German systems) to companies to enhance the safety of e-commerce transactions.

627 Office of the Privacy Commissioner *Privacy Impact Assessment Handbook* (2008).

628 See, for example, Immigration Act 2009, s 32.

629 Appendix 1, at [48].

630 Ibid, at [45].

631 Issues Paper at [Q159].

Submissions

10.49 There was a measure of support from 11 submitters. One submitter suggested that public sector agencies should be required to conduct PIAs. One submitter thought a PIA should be compulsory in relation to medical databases such as the B4 School Check. Some submitters commented on the resource implications of the proposal and others thought that the "significant impact" threshold would require clarification.

10.50 There was opposition to the proposal from five submitters on the basis that the Privacy Commissioner's current powers are sufficient to provide adequate incentives, new powers may make agencies reluctant to engage with OPC, and a best practice model is preferable.

10.51 The Privacy Commissioner favoured a new targeted reserve power to direct public sector agencies to produce PIAs in cases where she has significant concerns. The Privacy Commissioner advised us that such a power would have been useful on a number of past occasions to address systemic issues.

Our response

10.52 We agree that PIAs should continue to be promoted as a privacy design tool amongst both public and private sector agencies. Privacy Commissioner guidance and advice will remain crucial. In most circumstances we support the continuance of the voluntary compliance model, but consider that there is a case for public sector agencies to be required to produce a PIA in relation to initiatives that may impact on the handling of personal information. Citizens have little choice about their engagement with these agencies so there is a particular onus on them to observe best practice to ensure citizen trust in government.

10.53 There is a question of the form this mandatory requirement should take. We considered the option of giving the Privacy Commissioner a power to direct a core public sector agency to produce a PIA. The Australian Government has accepted a recommendation by the Australian Law Reform Commission to that effect.[632] However, we are reluctant to do anything which could prejudice the cooperation between public sector agencies and the Privacy Commissioner in relation to PIAs that currently exists and must continue. We think it constructive to retain OPC's role as one of guidance and encouragement in relation to PIAs.

10.54 Rather than create a new power of direction in OPC, we prefer the approach taken in the United Kingdom[633] and Canada,[634] which requires government departments to conduct PIAs as a matter of government policy. We think that such a requirement could best be achieved by a government policy decision

632 *For Your Information*, R47–4; *Enhancing National Privacy Protection*, at 86.

633 See Ministry of Justice (UK) "Undertaking Privacy Impact Assessments: the Data Protection Act 1998" (13 August 2010) < www.justice.gov.uk > .

634 See Government of Canada "Directive on Privacy Impact Assessments" (1 April 2010); "Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks" (31 August 2002) < www.tbs.gc.ca > ; Office of the Privacy Commissioner of Canada "Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada" < www.priv.gc.ca > .

communicated in a Cabinet Office circular rather than by a statutory provision. Cabinet Office circulars complement the Cabinet Manual and CabGuide, and provide detailed guidance on central government processes.

10.55 Such a policy should require, in the case of a proposal for legislation, that the regulatory impact statement incorporate a PIA where the proposal involves the handling of personal information, including a statement by the Privacy Commissioner on the adequacy of the assessment. It could also set out expectations that a PIA would be prepared where any proposed development has, or could have, significant implications for personal privacy. Examples might be developments involving a technology such as biometrics or radio frequency identification, or developments involving the sharing of personal information with other agencies or the sending of personal information offshore (through cloud computing, for example).

10.56 We recommend that the Government adopt such a policy and issue such a Cabinet circular. We also recommend that the State Services Commission provide guidance on its website as to expectations for use of PIAs in the public sector; such guidance should be prepared in consultation with the Department of Internal Affairs and the Privacy Commissioner.

RECOMMENDATION

R104 The Government should adopt a policy and issue a Cabinet Office circular setting out the circumstances in which public sector agencies are expected to produce a privacy impact assessment.

RECOMMENDATION

R105 The State Services Commission should provide guidance on its website as to expectations for use of privacy impact assessments in the public sector, such guidance being prepared in consultation with the Department of Internal Affairs and the Privacy Commissioner.

PARTICULAR TECHNOLOGIES

10.57 In the issues paper and the earlier study paper we outlined the impact of technological developments on the handling of personal information in a range of specific contexts including search engines and websites, social networking, cloud computing, deep packet inspection, location technologies, radio frequency identification and biometrics.[635] We also considered the growing practice of online tracking of website users to serve targeted advertising.[636] We asked if any of these specific technologies require any particular regulatory response, including legislative amendment.[637]

10.58 Overall, submitters generally did not support any specific reforms to the Privacy Act to respond to technological developments, preferring guidance from the Privacy Commissioner and, where necessary, best practice rules and consideration

635 Issues Paper at ch 13; Law Commission *Privacy: Concepts and Issues*, above n 561, at ch 6.

636 Issues Paper, at ch 15.

637 Ibid, at [Q160], [Q161], [Q169].

of a code of practice. The Privacy Officers Roundtable submitted that guidance from the Privacy Commissioner on specific topics or issues is always welcome and Telecom submitted that it would welcome general guidance about the practical implications of new technologies as they develop. The State Services Commission commented that the use of guidance and Privacy Commissioner codes is preferable to legislation in responding to new technologies, as legislation is more appropriate once a technology has matured and is better understood.

10.59 The Privacy Commissioner's own submission suggested that what is important is that the Privacy Act is sufficiently flexible to respond appropriately to whatever new technologies arise now and in the future, and that her Office has adequate powers to respond to new developments that pose threats to privacy. The Privacy Commissioner noted that guidance on some of the technologies highlighted in the issues paper may be useful.

Search engines, websites, social networking and online tracking

Submissions

10.60 Submissions on the topic of internet privacy noted the need for education. Telecom suggested that New Zealanders need to be educated that any information that is put online may end up being used for a different agenda. The Department of Labour suggested that the Privacy Commissioner could have a role in educating the public about privacy safety settings.

10.61 Another theme in submissions related to improving the effectiveness of privacy policies.[638] Noting the current information asymmetry and power imbalance between websites and their users in relation to privacy policies, one suggestion from the seminar on privacy and the internet organised for us by InternetNZ was that the Privacy Commissioner or another body could facilitate a process for model online terms and conditions.[639] Another suggestion was that the Privacy Commissioner or another body could consider facilitating the development of a Privacy Commons icon to represent complex privacy terms graphically.[640]

10.62 In relation to privacy issues between citizens that arise through internet publication, Professor Roth's submission, drawing from his academic article,[641] was that these issues are better covered by other causes of action such as defamation and the privacy tort and criminal offences such as computer misuse, rather than the Privacy Act. However, Roth notes that new remedies may be needed such as take down orders and time limits for removing information from web pages. Roth also notes that innovations in web design may enhance the protection of personal information on the internet.

638 For issues relating to privacy policies see United States Federal Trade Commission, above n 606, at 19, 70; Patrick Gage Kelley, Lucian Cesca, Joanna Bresee and Lorrie Faith Cranor "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach" in *Privacy Papers for Policy Makers 2009–2010* (Future of Privacy Forum, Washington, DC, 2010) 10.

639 InternetNZ Privacy Roundtables (Wellington, 21–22 June 2010).

640 See Tanzina Vega "Studies Find Success in Use of Privacy Icons" *New York Times* Media Decoder blog (16 November 2010) < http://mediadecoder.blogs.nytimes.com > .

641 Paul Roth "Data Protection Meets Web 2.0: Two Ships Passing in the Night" (2010) 33 UNSWLJ 532. For an illustration of these issues, see John Timpane "Dangers of a Big Brother Society" *Dominion Post* (Wellington, 2 October 2010) at A22.

10.63 Judge Harvey suggested that the offence of unauthorised access to a computer should be revised to delete section 252(2) of the Crimes Act 1961, which provides an exception to the offence where agency insiders access a computer system beyond the scope of their authority.

10.64 On the topic of online tracking and behavioural advertising, there was a range of responses, including:

- no response needed (2 submissions);
- wait and see before responding to the issues raised by this practice (2 submissions);
- undertake further work in this area (supported by the Marketing Association and the Ministry of Consumer Affairs);
- respond with Privacy Commissioner education and guidance (4 submissions);
- self-regulation (supported by Microsoft); and
- develop a code of practice (3 submissions).

Overseas developments

10.65 There is currently a great deal of study and policy consideration of online privacy issues being undertaken overseas, including:

- a review of the OECD Guidelines[642] (on which the New Zealand Privacy Act is based);[643]
- in Canada, public consultation by the Privacy Commissioner on topics including online tracking, profiling and targeting, and cloud computing;[644]
- in Europe, amendment of the ePrivacy Directive[645] with a requirement that the use of cookies be subject to users' opt-in consent,[646] and an impending review of the Data Protection Directive;
- in Australia, a Senate Standing Committee inquiry into the adequacy of privacy protections for Australians online;[647] and
- in the United States, the release of a preliminary report by the Federal Trade Commission,[648] a green paper by the Department of Commerce Internet Policy Task Force,[649] and a United States Senate Committee hearing on the use of location-based data.[650]

642 Organisation for Economic Co-operation and Development "The 30th Anniversary of the OECD Privacy Guidelines" < www.oecd.org/sti/privacyanniversary > .

643 Privacy Act 1993, long title.

644 Office of the Privacy Commissioner (Canada) *Consultations Report*, above n 603.

645 Privacy and Electronic Communications Directive 2002/58/EC [2002] OJ L201/37, amended by Directive 2009/136/EC [2009] OJ L337/11.

646 This is to be implemented by member countries by May 2011. See also Article 29 Data Protection Working Party *Opinion 2/2010 on Online Behavioural Advertising* (22 June 2010) 00909/10/EN WP 171.

647 Parliament of Australia, above n 610.

648 United States Federal Trade Commission, above n 606.

649 United States Department of Commerce Internet Policy Task Force *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (green paper, 16 December 2010).

650 United States Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy" (10 May 2011) < www.judiciary.senate.gov > .

10.66 In relation to online tracking for the purposes of serving targeted advertising, current developments include:

- the United States Federal Trade Commission preliminary staff report proposal for a "do not track" mechanism that would allow consumers to opt out of internet tracking,[651] and the introduction of a Bill to Congress that, if passed, would provide legislative authority for a "do not track" mechanism;[652]
- an Australian Senate Committee recommendation that the Australian Privacy Commissioner develop a code, in consultation with industry, that follows a "do not track" model;[653]
- the development of privacy products by the internet industry, such as anti-tracking tools for web-browsing software in Microsoft's Internet Explorer 9, Mozilla's Firefox 4 and Apple's Safari browser,[654] as well as other privacy services;[655] and
- the development of pictorial icons as an enhanced notification tool to inform web users about targeted advertising.[656]

10.67 In addition, there are continuing initiatives by advertising industry groups to develop self-regulatory measures for online behavioural advertising.[657] For example, IAB Europe has released a framework and the Australian Digital Advertising Alliance (ADAA) has released a best practice guideline, each laying down seven self-regulatory principles for industry when engaged in third party

651 United States Federal Trade Commission, above n 606.

652 "Do Not Track Me Online Act" HR 654 (introduced by Rep Jackie Speier). Other proposed do not track legislation includes a computer spyware bill (SB 761) introduced by Senator Alan Lowenthal in California (requiring regulations to allow web users to opt out of data collection and online tracking) and a Federal Bill introduced by Senator Jay Rockefeller as the Do-Not-Track Online Act of 2011 (S.913) (requiring the FTC to prescribe regulations for the use of personal information in online tracking). Further proposed US online privacy legislation includes the Commercial Privacy Bill of Rights Act of 2011 (S.799) sponsored by Senators Kerry and McCain (encouraging self-regulation but requiring an opt-in measure for the sharing of sensitive personal information and a clear and conspicuous mechanism allowing an opt-out from behavioural advertising); a Bill introduced by Rep Bobby Rush as the Best Practices Act of 2010 (requiring an opt-out option before sharing data with other companies); and a Bill sponsored by Rep Cliff Stearns and Rep Jim Matheson, introduced as the Consumer Privacy Protection Act of 2011 (HR 1528) (promoting industry self-regulation and requiring notification of data use).

653 Parliament of Australia, above n 610, recommendation 4.

654 Julia Angwin and Geoffrey A Fowler "Microsoft, Facebook Offer New Approaches to Boost Privacy" *Wall Street Journal* (26 February 2011) < http://online.wsj.com > ; Tony Bradley "Microsoft Web Privacy Clears W3C Hurdle" *PCWorld* (25 February 2011) < www.pcworld.com > ; Dan Misener "Do Not Track Me Online Please" *CBC News* (22 March 2011) < www.cbc.ca > ; Nick Wingfield "Apple Adds Do-Not-Track Tool to New Browser" *Wall Street Journal* (14 April 2011) < http://online.wsj.com > .

655 Julia Angwin and Emily Steel "Web's Hot New Commodity: Privacy" *Wall Street Journal* (28 February 2011) < http://online.wsj.com > .

656 Tim Bradshaw "Yahoo to Show How Data Used to Target Adverts" *Financial Times* (17 March 2011) < www.ft.com > ; Kate Kaye "Google, Yahoo and TRUSTe Advance Self-Reg Plans" *ClickZ* (22 March 2011) < www.clickz.com > ; IAB Europe *EU Framework for Online Behavioural Advertising* (27 April 2011) < www.iabeurope.eu > ; YourOnlineChoices "About ADAA" < www.youronlinechoices.com.au > . See also Digital Advertising Alliance *The Self-Regulatory Principles for Online Behavioural Advertising: Advertising Option Icon* < www.aboutads.info > .

657 For a discussion of other self-regulatory measures, see Issues Paper at ch 15.

online behavioural advertising across unrelated websites. These principles include notice, user choice, security safeguards, limits on advertising to children, education and accountability.[658]

Our response

Monitoring international reviews

10.68 We believe it is important for the Privacy Commissioner to continue to monitor overseas policy developments that relate to online privacy and to report on these developments to the extent that there may be implications for the online privacy of New Zealanders, or that they might provide a model approach that could be considered in New Zealand.

Education and guidance

10.69 We agree with submissions that the Privacy Commissioner's education function is critical in this context, and endorse the work of OPC to make information available on its website.[659] We note that user-education has also been recognised as a critical tool in Australia to ensure that people are equipped to protect their privacy online.[660] In the United Kingdom, the Information Commissioner's Office has produced a code of practice containing good practice advice for organisations that provide online services, a checklist for small businesses with an online presence and an information leaflet for consumers dealing with online personal information.[661]

10.70 While the exercise of the Privacy Commissioner's education function will involve the expenditure of resources in producing and disseminating information to New Zealanders in an effective way, we would expect that OPC will be able to continue to execute this function in a cost-effective manner in part by providing information on its website and by highlighting articles and other relevant materials produced by other Privacy Commissioners and Data Protection Commissioners, as well as by journalists, specialist websites and other organisations.[662]

10.71 We note the support in submissions for guidance from the Privacy Commissioner on technology topics and encourage OPC to continue its efforts in this area, subject to the overall priorities of the Office.

---

658 IAB Europe *EU Framework for Online Behavioural Advertising* (27 April 2011) < www.iabeurope.eu > ; Australian Digital Advertising Alliance *Australian Best Practice Guideline for Online Behavioural Advertising* (March 2011) < www.youronlinechoices.com.au > . Ten industry participants have signed up to the Australian code, including Google, Microsoft, Yahoo!7 and Fairfax Digital. See also Julian Lee "User-tracking Ads Guidelines Not Good Enough: Experts" *Sydney Morning Herald* (21 March 2011) < www.smh.com.au > .

659 See, for example, Office of the Privacy Commissioner "WiFi Tips" (2010) < http://privacy.org.nz/wifi-tips > .

660 Office of the Privacy Commissioner (Australia), above n 601, at 17.

661 Information Commissioner's Office (UK) *Personal Information Online Code of Practice*; *Small Business Checklist*; *Protecting Your Information Online* (2010).

662 See for example the *Wall Street Journal* "What They Know" series of articles on digital privacy (July – October 2010) < http://online.wsj.com/public/page/what-they-know-digital-privacy.html > .

10.72 The ALRC has also recommended that the Australian Privacy Commissioner should develop and publish guidance in relation to technologies that impact on privacy (such as data collecting software like cookies), and that this should include relevant local and international standards.[663]

Online privacy notices

10.73 We agree that online privacy notices pose real challenges for citizens. As summarised by the OECD:[664]

> Individuals may face a lack of information, or overly detailed information about how their personal information may be used. Individuals may find it difficult to assess information risks when confronted with complex information and competing interests. Further complications may arise when privacy policies change too frequently.

10.74 In Australia, a Senate Committee has recommended that the Australian Privacy Commissioner develop guidance on the appropriate use of privacy consent forms, and that the Commissioner's complaints-handling role be expanded to more effectively address complaints about the misuse of privacy consent forms in the online context.[665]

10.75 We agree that Privacy Commissioner should continue to take a leadership role in relation to the presentation of privacy notices, as priorities and resources allow.[666] It will be important for the Privacy Commissioner to continue to monitor initiatives to streamline and simplify online privacy notices (such as the use of icons).[667] In the meantime, we think that the Privacy Commissioner should consider providing or co-ordinating guidance to the public on navigating the privacy policies of heavily used websites such as Facebook.

10.76 One option that might be considered is creating an annual award for best privacy notice practice that could be awarded during Privacy Awareness Week. This could help raise awareness about privacy notices and encourage best practice. The opportunity could also be taken to draw attention to inadequate privacy notices.

10.77 We are not persuaded that the complaints-handling role of the Privacy Commissioner needs to be expanded (as has been recommended in Australia) to respond to issues with privacy notices. In our view, the Commissioner's powers and functions (as reformed in the ways recommended in this report) provide a range of options (such as investigation, public statement, education and compliance notice) depending on any particular circumstances.

---

663 *For Your Information* at R10–3. This recommendation has been accepted in principle: see *Enhancing National Privacy Protection* at 31.

664 Organisation for Economic Co-operation and Development *The Evolving Privacy Landscape: 30 Years After the OECD Guidelines* DSTI/ICCP/REG(2010)6/REV2, at 4–6.

665 Parliament of Australia, above n 610, recommendation 2.

666 The Office of the Privacy Commissioner's website provides information about privacy notices: "Questions and Answers About Layered Privacy Notices" (2008) < http://privacy.org.nz/effective-website-privacy-notices > .

667 For research on privacy policies see for example Kelley, Cesca, Bresee and Cranor, above n 638; Pedro Giovanni Leon, Lorrie Faith Cranor, Aleecia M McDonald and Robert McGuire "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens" (2010, CMU-CyLab-10-014).

Remedies or offences for online breaches between citizens

10.78 In relation to Paul Roth's submission relating to internet privacy issues between citizens, we are largely in agreement that no change to the Privacy Act is appropriate, although two changes we have recommended may be relevant in certain circumstances. First, we have recommended changes to the domestic affairs exception in section 56 of the Privacy Act. The recommended changes seek to narrow the scope of the domestic affairs exception, with the effect that grounds will exist to make a Privacy Act complaint for a breach of a privacy principle where information has been collected through misleading conduct or is obtained unlawfully or the collection, use or disclosure of the personal information would be highly offensive to a reasonable person.[668]

10.79 Second, we have recommended that the scope of the "publicly available publication" exception to principles 10 and 11 be narrowed so that it cannot be relied on if, in the circumstances, it would be unfair or unreasonable to use or disclose personal information obtained from a publicly available publication.[669]

10.80 We do not comment here about new remedies such as take down orders, other than to note the possibility of injunctive relief under the tort of invasion of privacy.[670] However, these are matters that we will consider in the Law Commission's New Media Project.[671]

10.81 In relation to the computer misuse offences and the reform suggested by Judge Harvey, we have previously recommended that there should be a separate review of the adequacy of these offences.[672] In the meantime, we continue to hold the view that "insiders" who access computer systems inappropriately should remain subject to civil law remedies such as the Privacy Act.[673] In chapter 3, we recommend that the Privacy Commissioner provide guidance on principle 5 and the issue of employee browsing of personal information.[674]

Online tracking

10.82 As noted above, it will be important for the Privacy Commissioner to monitor overseas developments, to keep the issue of online tracking under review and to report on this topic to government and to the public. In the meantime, we encourage the Privacy Commissioner to provide information and educational initiatives about online tracking, as resources and priorities allow.

10.83 We also encourage the Privacy Commissioner to consider the Marketing Association's proposal for a government/industry review committee with representatives from government, the information technology sector, the Marketing Association, the Advertising Standards Association, the Internet

668 R45.

669 R10.

670 *Hosking v Runting* [2005] 1 NZLR 1 (CA); see Law Commission *Penalties and Remedies,* above n 591, 148–149.

671 Law Commission "Review of Regulatory Gaps and the New Media" (Terms of Reference, 20 October 2010).

672 Law Commission, *Penalties and Remedies*, above n 591, at R3.

673 Ibid, at 111.

674 R15.

Advertising Bureau, InternetNZ, and NetSafe, to advise government on the appropriate form of regulation in this area to protect the interests of New Zealanders.[675]

Cloud computing

10.84 Cloud computing is described in the issues paper as the trend towards accessing computer and storage facilities from services on the internet, rather than using dedicated hard drives.[676] It has been billed as the next big thing in computing technology: "a technological and societal leap that will change how businesses function, how cities are planned, how people carry out their work and what citizens expect from online services."[677] Cloud computing involves an agency outsourcing data storage or processing to a provider who contracts to provide these services through the internet. There are significant cost savings and efficiency benefits to be achieved through the use of cloud services. However, careful consideration of the privacy and security issues is required where personal data is involved in the arrangement:[678]

> Adoption of broadband and the cloud – by both consumers and businesses – will be inhibited to the extent that there is a lack of trust; it's reasonable to expect that consumers and businesses will require a high level of confidence before they place sensitive financial or medical information in the cloud.

10.85 The Australian government has signalled that following recommendations of the ALRC, it intends to address privacy risks from businesses using cloud computing to store information in countries that have lower privacy standards than Australia does.[679] In New Zealand, the Privacy Commissioner has conducted a survey of the public and private sectors on the use of cloud computing, finding a need for guidance in both sectors.[680]

Submissions

10.86 A number of submissions addressed cloud computing. Telecom and Trade Me expressed the view that the Privacy Act is adequate to deal with cloud computing and the State Services Commission warned against changes that would cut New Zealand off from the potential benefits of cloud computing.

10.87 Microsoft suggested that the Privacy Commissioner have a specific function focussing on cloud computing that could emphasise the need to protect personal information held in the cloud, the need to monitor developments and to assist

675 The Marketing Association notes that a similar partnership between government and industry developed the regulatory framework for the Unsolicited Electronic Messages Act.

676 Issues Paper at [13.69].

677 Honor Mahony "EU gets to grip with cloud computing" *EUoberver* (5 April 2011) < http://euobserver.com > .

678 Julius Genachowski, Chairman of the US Federal Communications Commission, March 2011, cited in ibid. See also Fahmida Y Rashid "Epsilon Data Breach Highlights Cloud-Computing Security Concerns" (6 April 2011) < www.eweek.com > .

679 Renee Viellaris "Federal Government to Crack Down on Businesses Saving Data to the 'Cloud' Because of Privacy Concerns" *Sunday Mail* (Queensland, 3 April 2011) < www.news.com.au > .

680 Office of the Privacy Commissioner *International Disclosures and Overseas Information and Communications Technologies Survey* (May 2011).

the public to make informed choices. The State Services Commission suggested that the Privacy Commissioner's ability to engage and cooperate with overseas Privacy Commissioners and Data Protection Commissioners over complaints should be enhanced. The Department of Internal Affairs and the Privacy Commissioner suggested that guidelines on cloud computing may be needed.

Our response

10.88 We are concerned that the Privacy Act is not as clear as it might be in ensuring the accountability of agencies that take up cloud services to the individuals whose personal information is sent into the cloud. We think that accountability in this area should be clarified and in the following chapter we propose some changes to achieve this.[681] These include measures to improve cross-border enforcement cooperation between the New Zealand Privacy Commissioner and his or her overseas counterparts to facilitate cross-border complaints.

10.89 We do not recommend that the Privacy Commissioner have a specific function dedicated to issues relating to cloud computing. We are satisfied that the Commissioner's existing functions are sufficiently broad to allow him or her to highlight issues raised by cloud computing. We endorse the suggestion in submissions that cloud computing may be a strong candidate for additional guidance and note that this is a finding of the Privacy Commissioner's recent survey. Guidance would help to deliver the message that the take-up of cloud services needs to be properly structured so that privacy risks are addressed.[682] We also suggest that cloud computing may be a topic that could be addressed by an expert panel or by a Privacy by Design Panel.

Other technologies

10.90 In the issues paper, we discussed deep packet inspection, location technologies, radio frequency identification and biometrics. We received very few comments about these specific technologies in submissions to the issues paper.

Deep packet inspection

10.91 On the issue of deep packet inspection, submissions were received from internet service providers who supported the status quo under current legislation. Our analysis in the issues paper showed that deep packet inspection is subject to regulatory controls under the Telecommunications Information Privacy Code and under the Crimes Act, although some questions remain.[683]

681 R107–R115.

682 A clear and useful overview of the relevant security considerations is provided in Australian Government, Department of Defence, Intelligence and Security Cyber Security Operations Centre Initial Guidance "Cloud Computing Security Considerations" (12 April 2011) < www. dsd.gov.au > . See also Office of the Victorian Privacy Commissioner "Cloud Computing" Information Sheet (May 2011) < www.privacy.vic.gov.au > .

683 Issues Paper at [13.96]–[13.103].

10.92 We do not propose to make any recommendations on this topic, as it attracted little response in submissions. In our earlier report, we recommended that a separate review of data surveillance should be undertaken,[684] and this would be an opportunity to give further consideration to the regulation of deep packet inspection.

Location technologies

10.93 In relation to location technologies, there was support from InternetNZ and the State Services Commission for a new tracking device offence. We have recommended the creation of this offence in our earlier report.[685]

Radio frequency identification

10.94 On the topic of radio frequency identification, the State Services Commission suggested that new offences would be appropriate. However, no other submissions were received about this. In an earlier report, we noted that radio frequency identification could be included within the scope of a proposed tracking device offence.[686] In that report, we also recommended that the practice of RFID skimming should be considered as part of a broader review of the adequacy of New Zealand law to deal with data surveillance.[687]

10.95 We continue to hold the view expressed in our earlier report that radio frequency identification should also be regulated under the Privacy Act framework and that the Privacy Commissioner should continue to monitor this technology. At some future time the option of developing a code of practice may need to be explored.[688]

Biometrics

10.96 Few submissions commented on issues raised by biometrics. The Department of Internal Affairs suggested that some clarification of the handling of biometric information may be needed, and the State Services Commission requested that the issue of whether a biometric is a unique identifier be covered in any code of practice that may be issued in the future to cover biometrics. Another comment made to us expressed concern about inadequate controls on the use of biometric information and the risk from developing technology such as facial recognition. Concern was expressed about the potential for a person's image or other biometric information to be used as a unique identifier.

10.97 In chapter 3 we address questions about how biometric information should be handled under principle 12 (unique identifiers). Submissions did not support biometrics being treated as unique identifiers under principle 12 and we conclude that no change should be made in that regard. However, we think that the question of how to regulate biometrics within the privacy framework needs to be addressed. As we noted in the issues paper, the Immigration Act 2009

684 Law Commission *Penalties and Remedies*, above n 591, at R3.

685 Ibid, at R8.

686 Ibid, at [4.20].

687 Ibid, at [4.21].

688 Ibid, at R19.

specifically requires the collection and use of biometric information to be dealt with in accordance with the Privacy Act. It also requires a PIA to be carried out in respect of the handling of biometric information, in consultation with the Privacy Commissioner.[689]

10.98 We also noted that in Australia, the Biometrics Institute developed a Privacy Code which was then approved by the Australian Privacy Commissioner.[690] This Code incorporates higher standards of privacy protection for biometrics in certain areas, mandates the use of PIAs and specifies prevailing national and international standards to be observed.[691] Although the Code is not binding, except on the small number of member organisations that have subscribed to it, the Code is considered to provide a benchmark with requirements such PIAs becoming common practice.[692]

10.99 The Australian Biometrics Institute Privacy Code was reviewed in 2009. This review found that while the Code was considered by the industry to be an important step forward, its effectiveness was being hampered by underlying problems with the Australian privacy legislation. No changes to the Code have been made, pending implementation of the ALRC's recommendations for changes to the privacy legislation to address those issues.

10.100 Our preferred approach is that consideration be given to developing a New Zealand code of practice for biometric information. We are aware that the development of a code of practice can be a time-consuming and resource intensive; however, we think that this is an area where greater certainty and guidance would be useful. We also think that the process of developing a code could be streamlined by having regard to the Australian Biometrics Privacy Code as a model. It would be desirable for New Zealand and Australia to take a consistent approach to the treatment of biometrics under privacy legislation given the strong linkages between the Australian and New Zealand biometrics industries.[693] It would, however, be desirable to take account of any changes to the Australian Code that may be made following changes to the Australian privacy legislation. In the meantime, OPC could consider whether it is timely to provide guidance in this area.

RECOMMENDATION

R106 The Privacy Commissioner should consider whether it is timely to issue a code of practice or guidance covering biometrics.

689 Immigration Act 2009, ss 30–32; Issues Paper at [13.115].

690 Issues Paper at [13.114].

691 Office of the Privacy Commissioner (Australia) *Approval of Biometrics Institute Privacy Code* (Explanatory Statement, 2006); Biometrics Institute *Biometrics Institute Privacy Code* (2006).

692 The Code is binding on member organisations that have elected to subscribe to it and does not apply to government agencies. As at 10 January 2011, four member organisations have subscribed to the Code.

693 We note for example that the Biometrics Institute operates in both Australia and New Zealand.

Chapter 11

Sending personal information overseas

11.1 This chapter examines the situation where agencies collect personal information in New Zealand and then transfer that personal information to overseas destinations. We have not, in this context, dealt with the situation where New Zealand citizens send their own information offshore.[694]

NATURE OF THE PROBLEM

11.2 A recent Office of the Privacy Commissioner (OPC) survey of 50 New Zealand businesses and government agencies provides evidence of the growing trend for sending personal information to a variety of overseas countries.[695] The survey also highlighted that agencies do not consistently tell people that their information is being sent overseas, put controls on the further use of that information or check how the information is managed once it is sent overseas.

11.3 In the issues paper we discussed the huge increase since 1993 in the amount of personal information that is sent overseas.[696] We noted the growing use of cloud computing by agencies to outsource data processing and storage and assessed the operation of the Privacy Act framework in this context.[697] We considered the extent to which the transfer of personal information outside New Zealand may dilute or reduce privacy safeguards for that information.

11.4 Currently there is a risk that New Zealand agencies may send personal information to a country that does not have a privacy framework in place or without appropriate contractual provisions to ensure that privacy standards apply to protect the information following the transfer.

694 That situation raises a different range of cross-border issues, see Alan Toy "Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity" (2010) 24 NZULR 222. See also Parliament of Australia, Environment and Communications References Senate Committee *The Adequacy of Protections for the Privacy of Australians Online* (7 April 2011) at [3.87]–[3.95].

695 Office of the Privacy Commissioner *International Disclosures and Overseas Information and Communications Technologies Survey* (May 2011).

696 Issues Paper, at ch 14.

697 Ibid, at [13.69]–[13.86].

11.5 The key issues have been described by the Privacy Commissioner in the following terms:[698]

> It is increasingly difficult even to know where an individual's personal information is being held … [O]ne general trend has been plain to see for many years – that information freely travels about the globe as an integral part of the new economy… Much of this innovation and rapid data exchange is great news for individuals, business, government and the economy generally…. However, there are many challenges as well. One of these is the regulatory challenge of protecting personal information consistent with generally agreed international principles and, in New Zealand's case, the Privacy Act 1993…. For example, how can the law ensure that New Zealanders' information is adequately protected when sent offshore for processing? How can our trading partners be sure that their information is safe when sent here for processing? How can New Zealanders exercise their rights of access and correction when information is held in another country? What can be done when an agency's actions breach an individual's privacy? New Zealanders want their personal information protected wherever it travels.

11.6 In the issues paper we asked whether there should be more protections around personal information being sent out of New Zealand.[699] An amendment to the Privacy Act was enacted in 2010 to allow the New Zealand Privacy Commissioner to exercise intervention powers in relation to international data transfers. These powers relate to situations in which New Zealand is used as a conduit for transfers of personal data from overseas to destinations without adequate privacy frameworks in place.[700] The key benefit of the amendment to New Zealand is that it removes an obstacle to New Zealand achieving EU adequacy status (that is, being assessed as providing an adequate level of protection for personal data transferred from EU Member States for the purposes of the EU Data Protection Directive).[701] This is expected to open up new trading opportunities, for example in data processing, cloud computing and financial or call centre activity.[702] In privacy terms, however, the amendment primarily benefits citizens of New Zealand's overseas trading partners and does not address concerns about transfers of data that originate in New Zealand to destinations that lack adequate privacy standards.

698 Office of the Privacy Commissioner *Annual Report 2010* (Wellington, 2010) at 25 [*Annual Report*].

699 Issues Paper at [Q162].

700 The Privacy (Cross-border Information) Amendment Act 2010 came into force on 8 September 2010.

701 The Article 29 Data Protection Working Party has issued an opinion assessing New Zealand as having an adequate level of protection for purposes of the Data Protection Directive: *Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand* (4 April 2011) 00665/11/EN WP 182. See also Office of the Privacy Commissioner "NZ Data Protection Law Gets Tick From EU Committee" (press release, 13 April 2011).

702 Office of the Privacy Commissioner *Annual Report*, above n 698, at 13.

THE APPROACH TO REFORM

Submissions

11.7 In responding to the question about whether there should be more protections around personal information being sent out of New Zealand, nine submitters supported the introduction of more protections in the Privacy Act, while five submitters were happy with the status quo. Three government agencies (Inland Revenue, the Ministry of Social Development and the Customs Service) noted that they have specific statutory provisions authorising cross-border information sharing in certain circumstances.

11.8 Of those submitters who supported additional measures, five supported measures based on the accountability model discussed in the issues paper (that is, where the onus is on an agency to make appropriate arrangements for the protection of personal information it sends overseas).[703] In its submission, OPC noted the advantages of an accountability model for New Zealanders if they can look to the local agency they deal with to look after their information and hold that agency accountable. Google submitted that the accountability model should include a number of exceptions such as consent, comparable privacy laws in the destination jurisdiction, where the transfer is required or authorised by law (including law enforcement requirements in the destination jurisdiction), and for reasons of health and public safety. The Commerce Commission supported a hybrid of the data export controls model (which prohibits the export of data to a country without similar data protection standards) and the accountability model.

11.9 At the forum organised for us by InternetNZ,[704] concern was expressed about the potential breadth of the scope of section 10(3) of the Privacy Act,[705] which provides an exception to accountability where personal information is disclosed in order to comply with the requirements of a foreign law (such as the USA PATRIOT Act).[706]

Our response

11.10 Agencies send personal information overseas through a variety of transactions ranging from:

- the outsourcing of personal information for processing or storage to an overseas agency which acts as the agent of the New Zealand outsourcer and is restricted from using the personal information for purposes other than those related to the outsourcing, to
- the disclosure of personal information to an overseas agency for its own use.

703 Issues Paper at [14.45], [Q163].

704 InternetNZ Privacy Roundtables (Wellington, 21–22 June 2010).

705 See n 709 below.

706 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. See Gehan Gunasekara "The 'Final' Privacy Frontier? Regulating Trans-border Data Flows" (2006) 15 IJLIT 362 at 374–378.

Taking account of this spectrum of transactions from outsourcing to disclosure has been a critical factor in our analysis. We have concluded that, while an agency should be accountable for sending personal information overseas, the level of accountability should depend in each case on the type of transfer involved.

11.11 First, the level of accountability on an agency outsourcing personal information overseas should be relatively strong. This is consistent with the law of principal and agent, where a principal is responsible for the actions of its agent. In our view, it is appropriate for an agency taking a business decision to outsource the processing of personal information to another entity, to remain fully accountable for the handling of that personal information. This is on the basis that people who entrust their personal information to an organisation should not be disadvantaged in privacy terms by the outsourcing decision. In practice, this means that outsourcing arrangements must ensure that the personal information will be subject to privacy standards of a comparable kind to the New Zealand Privacy Act. This is the level of accountability we think is intended by the Privacy Act; however, we believe that the current provisions could be clarified.

11.12 Secondly, in relation to other disclosures overseas, we think that accountability should be of a different and more limited kind. The disclosing agency should be accountable for compliance with the privacy principles. Any disclosure which was not in conformity with principle 11 would itself be a breach by the disclosing agency. In addition, we think the agency should be required to take reasonable care that information disclosed overseas will be subject to acceptable privacy standards. We recommend amendments to the Privacy Act to introduce this new requirement. Our preferred model is in effect a hybrid model that encompasses both accountability and elements of a data export controls model, but only to the extent that this does not impact unduly on the global free flow of information.

11.13 We view the proposed changes as important measures to ensure more consistent privacy protection of the personal information of New Zealanders, regardless of where that information ends up being held or who ends up holding it.

11.14 In terms of the substance of the amendments that should be made, we assessed whether this should be done by introducing a new accountability principle into the Act's information privacy principles.[707] While this was supported by OPC, no further support for this option was expressed in submissions. On this basis, we do not believe that there is sufficient support for a new principle. We have therefore considered other specific amendments that could be made to the Privacy Act to strengthen accountability.

11.15 While existing measures in the Privacy Act go some way towards protecting personal information sent out of New Zealand and holding agencies accountable, the current provisions are dispersed and we think they need to be updated, clarified and consolidated in one part of the Act. To apply the Privacy Act

707 Issues Paper at [4.126], [Q60].

framework to cross-border data transfers, an agency currently has to navigate section 3(4),[708] section 10,[709] principles 5(b), 10 and 11, and new Part 11A. In our view, this exercise is unduly complicated.

11.16 We also think that these provisions could go somewhat further than they currently do in promoting accountability. We now deal separately with the two types of situation we have identified.

OUTSOURCING PERSONAL INFORMATION OVERSEAS

11.17 Where an agency outsources the processing of personal information by using an overseas agency to carry out the processing on its behalf,[710] for example through cloud computing, the Privacy Act treats the outsourcing agency as still holding the personal information (and therefore being accountable for it), even though it has been sent overseas for processing by another agency.[711]

11.18 The current provisions do not anticipate the complexity and sophistication of contractual cloud computing arrangements or the cross-border nature of outsourcing arrangements that are now entered into. One issue is that section 3(4) of the Privacy Act, which confirms an agency's accountability for personal information that it has outsourced (by deeming it still to be held by the outsourcing agency), also has the function of exempting a service provider from accountability. The condition for this exemption is that the service provider does not use or disclose the information for its own purposes. The structure of the provision, however, means that non-compliance with that condition by the service provider will result in the information no longer being deemed to be held by the outsourcing agency, and therefore dilutes that agency's level of accountability. In our view, the dual functions of section 3(4) should be dealt with separately. The condition should only act to exempt the service provider from accountability. It should not serve to limit the accountability of the principal agency.

708 Section 3(4) of the Privacy Act provides:

> For the purposes of this Act, where an agency holds information—
>
> (a) solely as agent; or
>
> (b) for the sole purpose of safe custody; or
>
> (c) 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 shall be deemed to be held by the agency on whose behalf that information is so held or, as the case may be, is so processed.

709 Section 10 of the Privacy Act provides:

> (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.
>
> (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.

710 The Canadian Privacy Commissioner, in guidelines about processing personal data across borders, describes a transfer of personal information for processing as a "use" by an organisation rather than a "disclosure": Office of the Privacy Commissioner (Canada) *Processing Personal Data Across Borders* (2009).

711 Privacy Act 1993, s 3(4), s 10(1), (2).

11.19 While the structure of section 3(4) may not create any particular difficulties in a domestic context, as both the outsourcing agency and the service provider will be subject to the New Zealand Privacy Act, it becomes more problematic to apply New Zealand privacy safeguards where the service provider is an overseas entity. Cross-border outsourcing therefore strengthens the rationale for the outsourcing agency to remain accountable for the handling of the personal information under that arrangement.

11.20 We recommend that a broader accountability provision be introduced in relation to transfers for the purposes of outsourcing, along the lines of a provision in the Canadian Personal Information Protection and Electronic Documents Act 2000 (PIPEDA):[712]

> An agency is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.

The new provision should capture the range of agency functions currently within the scope of section 3(4), including safe custody and processing.

11.21 The adoption of a provision of this sort would simplify and clarify the current approach under section 3(4) of the Privacy Act. It would mean that an agency will be responsible and answerable for any privacy breach by the service provider under outsourcing arrangements.

11.22 A strict accountability requirement of this kind means that to protect itself, an agency needs to engage in a risk assessment exercise prior to outsourcing personal data overseas and take any necessary steps to mitigate any identified risks that may expose an agency to liability for the acts of its service provider. The PIPEDA provision cited above spells this out explicitly in the statutory provision by requiring an agency to "use contractual or other means to provide a comparable level of protection while the information is being processed by a third party". We assessed this aspect of the PIPEDA model but conclude that within the scheme of the New Zealand Privacy Act, a requirement of this sort is more appropriately a matter for guidance than a statutory requirement.

11.23 Our preferred approach is for the principle of responsibility to be stated in the Privacy Act. It means in effect that the agency which outsources work is accountable under the Act if anything goes wrong. The Privacy Commissioner should provide guidance as to how outsourcing agencies can protect themselves by using contractual or other means to ensure a comparable level of protection to the Privacy Act for outsourced data.

11.24 As part of such guidance, the Privacy Commissioner could consider whether it would be helpful for agencies if OPC maintained a list of jurisdictions that have implemented comparable privacy standards to the New Zealand Privacy Act. While this would not create an approval for any particular outsourcing arrangement, it would provide agencies with some assurance in selecting jurisdictions for outsourcing purposes. Where a jurisdiction is not included on the Privacy Commissioner's list, this would indicate to agencies that further

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

measures such as contractual provisions may be needed before outsourcing to that jurisdiction, in order to meet the accountability standard under the Privacy Act.

11.25 We are not proposing that there would be any exceptions to this accountability provision, other than the exception in section 10(3) of the Privacy Act that exempts any action required by the law of a foreign jurisdiction. While this exception introduces the potential for the dilution of privacy protection by the override of other laws, we think that it would be difficult to remove it. It represents the foreign equivalent of section 7 that allows New Zealand laws to override the privacy principles.

11.26 Where there are significant concerns about a foreign law requirement, this could be a matter for comment or guidance from the Privacy Commissioner. Such guidance could inform the public and agencies about the existence of the requirement that may impact on the privacy protection of personal information transferred to that jurisdiction, as well as options for agencies to consider before making transfers. Notification of foreign law requirements at the time a person's data is collected may also go some way towards reducing concern about their impact.[713]

11.27 It is important to note that this form of accountability would be limited to cross-border outsourcing arrangements and would not apply to other cross-border transfers of personal information. We recommend a different accountability standard for those other disclosures of personal information overseas.[714]

RECOMMENDATION

R107 The Privacy Act should include an express statement of full accountability for cross-border outsourcing arrangements. It should be based on the first part of the Canadian Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) provision to the following effect:

> An agency is responsible for personal information it holds, including information that has been transferred to a third party for storage, custody or processing.

RECOMMENDATION

R108 The Privacy Commissioner should provide guidance for agencies on conducting risk assessment prior to outsourcing personal information overseas and on the use of contractual or other means to ensure the application of privacy standards of a kind comparable to the New Zealand Privacy Act.

713 See Gunasekara, above n 706, at 384–385.

714 See R110.

Domestic outsourcing

11.28 Our preference is for all provisions relating to cross-border transfers to be located in one part of the Privacy Act. Consideration will need to be given to allocating accountability for domestic outsourcing arrangements (currently in section 3(4)). We recommend that this be done consistently with the allocation of accountability for cross border outsourcing arrangements, by enacting a parallel provision that would apply to domestic arrangements.

RECOMMENDATION

R109 The Privacy Act should include an express statement of full accountability for domestic outsourcing arrangements, as a parallel provision to that recommended in R107.

OTHER OVERSEAS DISCLOSURES

11.29 Where a New Zealand agency discloses personal information it holds to an overseas entity for that entity's own use and further disclosure, the Privacy Act requires the initial disclosure to the overseas entity to comply with principle 11, but at present that is the extent of the disclosing agency's accountability. There is no requirement in the New Zealand Privacy Act for the disclosing agency to consider whether the information will receive adequate protection once it reaches the overseas destination. Where the disclosure is between New Zealand entities, any further use and disclosure by the receiver of the information will be governed by the New Zealand privacy principles. However, the overseas recipient of personal information will generally be outside the Privacy Act's territorial jurisdiction, although the recipient may be subject to the Privacy Act if it is an entity that carries on activities in New Zealand.[715] Where the information receiver is beyond the jurisdiction of the Privacy Act, the extent of any privacy safeguards will depend on any other applicable privacy framework. In the issues paper, we identified this as a potential gap in the law.[716]

11.30 We recommend an express requirement for the disclosing agency to take any reasonable steps that may be necessary to ensure that the personal information will be subject to acceptable privacy standards (either by law, contract or binding scheme) following the disclosure overseas.

11.31 To identify what reasonable steps are required would require an agency to engage in a risk-assessment exercise prior to disclosure to consider whether any statutory or other framework would apply privacy standards to the personal information following its transfer. If not, the agency should then identify the steps required to structure the disclosure (such as through contractual arrangements) to ensure that privacy protection is operative.

715 Toy, above n 694, at 225, 233–234.

716 Issues Paper at [14.38].

11.32 This accountability measure would apply to any cross-border disclosure of personal information by one agency to an overseas agency, such as the disclosure of personal information by one business to another business overseas for its own use, or the transfer of personal information between affiliates or different offices of a multinational corporation. We also propose a range of exceptions.[717]

11.33 "Acceptable privacy standards" need not necessarily be identical to the New Zealand Privacy Act. "Acceptable privacy standards" should include standards based on recognised international instruments such as the OECD basic principles of national application,[718] the EU Directive[719] or the APEC Privacy Framework principles.[720] They could have application to the transaction either by the law of the overseas country, or by contract or other binding scheme entered into by the parties. The Privacy Commissioner should be empowered to approve the international privacy frameworks which are regarded as acceptable for this purpose.

11.34 We think that the Privacy Commissioner should provide guidance for New Zealand agencies on conducting risk assessments prior to disclosing personal information overseas and the use of contractual or other means to ensure acceptable privacy standards are in place. As part of such guidance, the Privacy Commissioner could consider whether it would be helpful for agencies if OPC maintained a list of jurisdictions that have implemented acceptable privacy standards based on one of the approved international privacy frameworks.

Exceptions

11.35 Exceptions to this accountability provision should include disclosures:

- to the individual concerned;
- where necessary to avoid prejudice to the maintenance of the law; or
- where necessary to avoid a serious threat to public health or safety, or to the life or health of an individual.

11.36 In addition, the exception currently contained in section 10(3) for disclosures required by the laws of a foreign country should continue to apply. Further, section 7 of the Privacy Act would recognise that specific legislation may create additional exceptions for disclosures of personal information overseas by particular agencies.

11.37 A further exception would be needed to exclude disclosures made in a "publicly available publication"[721] such as a book, magazine, newspaper, public register, or website.[722] This is because the intent of the new accountability provision is not to limit disclosures to the world at large, but rather to protect targeted disclosures of personal information between agencies. We discuss below the imperative to avoid undesirable limits on the free flow of information.

---

717 See [11.35]–[11.38].

718 The OECD principles are contained in sch 5A to the Privacy Act 1993.

719 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.

720 For an overview of the international instruments see Issues Paper at [14.8]–[14.27].

721 Privacy Act 1993, s 2(1).

722 See recommended amendments to the definition of "publicly available publication", R8.

11.38 We considered whether an individual's consent to an overseas disclosure should be a further exception but do not recommend this. We think that meaningful consent would be unwieldy and difficult to achieve in a way that is both readily understandable for individuals[723] and efficient and cost-effective for agencies. The intent is that consent would remain an exception to the prohibition on disclosure under principle 11(d), but would not exempt an agency from complying with the accountability requirement to ensure acceptable privacy standards apply following the disclosure.

Hybrid model

11.39 While our recommended approach to overseas disclosures is based on an accountability model (where the onus is on an agency to make appropriate arrangements for the protection of personal information it sends overseas) it also contains elements of a data export controls model (which prohibits the export of data to a country without similar data protection standards).[724] We think that a hybrid model offers an opportunity to achieve a balance between the benefits and disadvantages of each model in its pure form.[725]

11.40 One issue with the data export controls model is its potential to impede the free flow of data. The general desirability of the free flow of information to promote global trade is a matter that needs to be balanced against privacy protection under international instruments such as the OECD Guidelines, the EU Directive and the APEC Privacy Framework.[726] We have therefore been careful to frame the accountability provision for overseas disclosures sufficiently broadly so as not to unduly limit transfers of personal information.

11.41 First, the recommended provision would not impose strict accountability on an agency disclosing personal information overseas for privacy breaches by the recipient of the information, as we think this could act as an undesirable limit on the free flow of information.[727]

11.42 Secondly, we think that a data export controls model that would set the New Zealand privacy principles as a minimum benchmark would be overly burdensome and unduly restrictive.[728] We do not think this approach can be justified as a general condition of disclosure overseas, when balanced with the

723 See Gunasekara, above n 706, at 381.

724 See Christopher Kuner "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future" (*Tilburg Institute for Law, Technology and Society Law & Technology Working Paper* No 016/2010) at 7, 40.

725 The perceived disadvantages are uncertainty (in the case of the accountability model) and inflexibility (in the case of the data export controls model).

726 See, for example, Privacy Act 1993, s 14(a), s 114B(2)(b); Blair Stewart "The Economics of Data Privacy: Should We Place a Dollar Value on Personal Autonomy and Dignity?" (paper presented to the 26th International Conference of Privacy and Data Protection Commissioners, Wroclaw, Poland, 15 September 2004).

727 This is in contrast to the proposed standard of accountability for outsourcing arrangements, where an outsourcing agency would be accountable for privacy breaches by its service provider.

728 For example, the option of requiring "comparable safeguards" to the Privacy Act is a model used in the Privacy Act 1993, s 114B(1)(a), and in Australian Government "Exposure Draft: Australian Privacy Principles" principle 8(2)(a)(i).

general desirability of the free flow of information.[729] Nevertheless, we believe that some minimum standard of privacy protection is required as a condition of exporting personal information from New Zealand. We therefore propose that any privacy framework based on internationally accepted privacy values, while not identical to the New Zealand privacy principles, should be considered acceptable for the purposes of overseas disclosures of personal information. The advantage of setting a flexible benchmark is that it avoids imposing a barrier to cross-border data flows on countries that have implemented privacy laws in accordance with international instruments.

11.43 Where there is no generic privacy framework in place, this will not necessarily prevent overseas disclosures, if the transferring and receiving agencies establish an appropriate framework by contract. Another potential mechanism to facilitate overseas disclosures would be through cross-border privacy rules, which we discuss below.

11.44 We have considered the proposed Australian approach to accountability for cross-border disclosures, which is also a hybrid of the accountability and data export controls models. Draft Australian Privacy Principle 8 would require an Australian entity disclosing personal information to an overseas entity to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian privacy principles in relation to the information. Accountability is further strengthened through section 20 of the Exposure Draft, which provides that the Australian entity is to be responsible for acts by the overseas entity that would be in breach of the Australian privacy principles. However, there has been criticism of the Australian principle for the large number of exceptions to this accountability measure.[730] A Senate Committee has recommended that the Australian provision be amended to strengthen accountability for offshore disclosures of personal information.[731]

11.45 Rather than setting up a broad accountability measure that is subject to numerous exceptions along the lines of the Australian provision, our preferred approach is a more targeted provision. As noted above, we also prefer a more flexible approach that recognises the legitimacy of privacy frameworks that are not necessarily identical to New Zealand's privacy principles but which are based on a recognised set of privacy values.

RECOMMENDATION

R110 A new accountability measure should be introduced for disclosures of personal information overseas (other than outsourcing arrangements). Disclosing agencies should be required to take such steps as may be reasonably necessary to ensure that the information disclosed will be subject to acceptable privacy standards.

729 See *Necessary and Desirable* at [2.18.20] proposing a transborder data flow control at the "weaker" end of the scale so as not to create excessive or unnecessary barriers to transborder data flows.

730 Australian Government, above n 728, principle 8(2).

731 Parliament of Australia, above n 694, at [3.109].

RECOMMENDATION

R111 Exceptions to the new measure should include disclosures:

- to the individual concerned;
- where necessary to avoid prejudice to the maintenance of the law;
- where necessary to avoid a serious threat to public health or safety or to the life or health of an individual; or
- made in a publicly available publication.

Sections 7 and 10(3) (or their replacements) should apply to the new measure.

RECOMMENDATION

R112 The Privacy Commissioner should have power to approve specified overseas privacy frameworks as providing acceptable privacy standards. The Office of the Privacy Commissioner should maintain a list of such frameworks on its website.

RECOMMENDATION

R113 The Privacy Commissioner should provide guidance for New Zealand agencies on conducting risk assessment prior to disclosing personal information overseas and on the use of contractual or other means to ensure the application of acceptable privacy standards.

DATA TRANSFER PROHIBITION POWERS

11.46 The Privacy (Cross-border Information) Amendment Act 2010 has empowered the Privacy Commissioner to block transfers of personal information or impose conditions on the transfer of personal information. The Commissioner can do so if he or she is satisfied that the information is likely to be transferred to a destination that does not observe comparable privacy safeguards to the Privacy Act, and the transfer would likely lead to a contravention of the OECD basic principles of national application.[732] However, this power is only exercisable in relation to personal information that has been received in New Zealand from another State and which is then to be transferred on.[733] The Privacy Commissioner has issued a fact sheet explaining how the powers in Part 11A are intended to be used, which indicates that they will not be exercised lightly.[734]

732 Privacy Act 1993, s 114B. The Privacy Commissioner must also take account of other considerations such as whether the transfer would be likely to affect an individual, the desirability of encouraging free flows of information between New Zealand and other States, and any other international guidelines.

733 Privacy Act 1993, s 114B(1)(a).

734 Office of the Privacy Commissioner *Fact Sheet on Part 11A of the Privacy Act: Transfer of Personal Information Outside New Zealand* (2010).

11.47 In relation to transfers of information originating in New Zealand, we have explained above that we believe an accountability model is best at the present time. This imposes a duty on the agency sending information abroad to take care that the overseas recipient will observe appropriate privacy standards. However, there may be cases where an agency does not observe these due diligence requirements, and where information is sent to destinations which are "privacy unsafe".

11.48 We have wondered whether the Privacy Commissioner's data transfer prohibition powers under the 2010 amendment should be extended to empower the Commissioner to block the transfer of New Zealanders' information out of New Zealand in such a case. At first sight this seems logical: why should the Commissioner be limited to using this enforcement tool only in relation to transfers that use New Zealand as a conduit?

11.49 However, we do not think such an extension is necessary. We have recommended in chapter 6 that the Commissioner should have a general power to issue compliance notices.[735] If information is being sent, or is about to be sent, overseas in breach of principle 11 or in breach of the due diligence obligations we propose, the agency concerned would be failing to comply with the requirements of the Privacy Act. In that circumstance we believe it would be appropriate for the Commissioner to exercise the power to issue a compliance notice. We prefer, therefore, not to make any amendment specifically directed at data transfer prohibition. We emphasise that we do not suggest that there should be any change to the provisions introduced by the 2010 Amendment Act.

11.50 If our recommendations about compliance notices are not accepted, however, we believe consideration should be given to the extension of the Commissioner's data prohibition notice powers.

CROSS-BORDER ENFORCEMENT COOPERATION

11.51 A particular priority of OPC has been to enhance or create mechanisms to promote cooperation between privacy enforcement agencies. The Office reports that it played a key role in two new initiatives:[736]

- the establishment of the APEC Cross-border Privacy Enforcement Arrangement, which aims to establish a framework for regional cooperation in the enforcement of privacy laws; and
- the Global Privacy Enforcement Network (GPEN), established in cooperation with an OECD working party.[737]

735 See R63.

736 Office of the Privacy Commissioner *Annual Report*, above n 698, at 26.

737 The participating GPEN privacy enforcement authorities include the US Federal Trade Commission; the Offices of the Privacy Commissioners of Canada, New Zealand, Australia (Federal), and Victoria; the Offices of the Data Protection Commissioners of Italy, Spain, Germany, the Netherlands and Ireland; the UK Information Commissioner; the French Commission Nationale de l'Informatique et des Libertés; and the Israeli Law, Information and Technology Authority: Global Privacy Enforcement Network "Action Plan for the Global Privacy Enforcement Network (GPEN)" (2009) < www.privacyenforcement.net > .

11.52 The Privacy Act already provides for a measure of cooperation with other authorities and stakeholders. The Privacy (Cross-border Information) Amendment Act 2010 introduced section 72C, which allows the Privacy Commissioner to consult with overseas privacy enforcement authorities about specific complaints and refer complaints or parts of complaints to those authorities where appropriate.

11.53 In the issues paper we asked whether the Act should be further amended to implement the broader cooperation measures contained in the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy,[738] to enhance the Privacy Commissioner's powers to work with his or her overseas counterparts in enforcing privacy safeguards in cases that involve parties spread across different jurisdictions.

11.54 Submissions supported the further cooperative measures that were outlined in the issues paper:[739]

- enabling the Privacy Commissioner to share relevant information with overseas privacy enforcement authorities relating to possible violations of privacy law;[740]
- enabling the Privacy Commissioner to provide assistance to overseas authorities relating to possible violations of the overseas country's privacy law;
- permitting requests for and provision of mutual assistance between the Privacy Commissioner and his or her overseas counterparts;
- providing for cooperation with other authorities and stakeholders; and
- supplementing the Tribunal's procedural powers to deal with cross-border privacy complaints.

11.55 We recommend that these measures should now be implemented in a manner broad enough to allow the Privacy Commissioner to liaise not only with his or her statutory counterparts, but also with private sector accountability agents that will be a feature of the cross-border privacy rules system discussed below. We note that in Canada, a new provision has recently been added to PIPEDA, allowing the Canadian Privacy Commissioner to share information with the Commissioner's foreign counterparts and other persons or bodies that have responsibilities for privacy breaches. Such information can be shared if it is relevant to a foreign investigation into breach of privacy laws.[741]

738 Issues Paper at [Q164].

739 Ibid, at [14.63].

740 See Office of the Privacy Commissioner "Report by the Privacy Commissioner to the Minister of Justice on the Privacy (Cross-border Information) Amendment Bill" (1 July 2009) at [2.7]–[2.8].

741 Personal Information Protection and Electronic Documents Act SC 2000 c 5, s 23.1.

11.56 We see enhancement of the Privacy Commissioner's cooperation powers as a useful response to the particular challenges of enforcing privacy protection in an online environment.

RECOMMENDATION

R114 The Privacy Act should be amended to:

- enable the Privacy Commissioner to share relevant information with overseas privacy enforcement authorities relating to possible violations of privacy law;
- enable the Privacy Commissioner to provide assistance to overseas authorities relating to possible violations of the overseas country's privacy law;
- provide for requesting and giving mutual assistance between the Privacy Commissioner and his or her overseas counterparts;
- provide for cooperation with other authorities and stakeholders; and
- supplement the Tribunal's procedural powers to deal with cross-border privacy complaints.

APEC CROSS-BORDER PRIVACY RULES

11.57 In the issues paper we discussed the system of cross-border privacy rules (CBPR) being developed under the APEC Privacy Framework so that agencies operating across a number of jurisdictions can opt to make their businesses subject to a uniform set of privacy rules. We asked whether there is value in implementing this system in New Zealand.[742]

11.58 Nine submissions responded to this question. Six submissions expressed a measure of support. Two submissions expressed reservations about cost and complexity. Of the submissions in support that addressed the point, all suggested that OPC would be the appropriate enforcement agency in such a system.

11.59 OPC felt it difficult to give a definite answer to the question posed, since final documentation is in the process of being completed by APEC, although OPC confirmed that most of the documentation is now available. The view of the Privacy Commissioner is that the most flexible approach would be to pass amendments to the Privacy Act to allow for the recognition of cross-border privacy rules, as this is an initiative that is likely to assume greater relevance in the medium term. This would not commit New Zealand to adopting the CBPR system but would create an opportunity to for New Zealand to opt in to the system, should it be considered advantageous to do so in the future.

742 Issues Paper at [Q165].

11.60 We agree that the opportunity should be taken to make any necessary changes to the Privacy Act to anticipate this development. The Privacy Commissioner should be provided with the prospective power to participate in a CBPR system or to establish accountability agents. The CBPR system would assist to address gaps in privacy coverage exposed by the globalisation of information flows and may prove to be a useful additional mechanism for agencies to use to meet the proposed accountability standards for cross-border transfers.

RECOMMENDATION

R115 The Privacy Act should include a provision allowing for the future adoption of a cross-border privacy rules system in New Zealand. The provision should come into force at a time to be determined by Order in Council.

Chapter 12
Other issues

12.1 This chapter discusses a number of specific issues not discussed elsewhere in the report:

- direct marketing;
- identity crime;
- culture and privacy;
- children and young people;
- other people with specific needs, particularly individuals with reduced capacity;
- workplace privacy;
- health information; and
- privacy officers.

DIRECT MARKETING

12.2 In the issues paper, we examined direct marketing and the relation of the Privacy Act to it. We asked if any changes to the Privacy Act are needed to regulate any particular form of direct marketing.[743]

Submissions

12.3 There was a mixed response from submitters. Five submitters supported the status quo. Most responses supporting any change were concerned particularly with telemarketing.

Direct marketing and the Privacy Act

12.4 The Commerce Commission supported a new direct marketing principle in the Privacy Act that would allow people to opt out of receiving direct marketing from an organisation, on the basis of harmonisation with Australia.[744] An express right to opt out of direct marketing in the Privacy Act was also supported by the Office of the Privacy Commissioner (OPC), the Advertising Standards Authority and the Marketing Association. Otherwise, however, the Marketing Association was opposed to including further controls on marketing

743 Issues Paper at ch 15.

744 Privacy Act 1988 (Cth), sch 3, NPP 2.1(c); Australian Government "Exposure Draft Australian Privacy Principles", principle 7 – direct marketing.

in the Privacy Act, suggesting that if any further controls are to be considered, the Fair Trading Act 1986, the Unsolicited Electronic Messages Act 2007 and the Telecommunications Act 2001 would be more appropriate legislative vehicles.

12.5 Professor Paul Roth supported implementation of the Privacy Commissioner's recommendation from *Necessary and Desirable* that principle 7 be amended to provide for a right of individuals to prevent the use of personal information for direct marketing purposes through deletion or blocking.[745]

12.6 The New Zealand Law Society suggested that marketing issues could be dealt with in a Privacy Act code of practice or Privacy Commissioner guidance, but noted that it is important not to confuse wider consumer issues (such as misleading or deceptive conduct) with privacy issues. The Privacy Commissioner noted that her code-making powers would likely need to be supplemented if direct marketing were to be covered in a code of practice.

Do Not Call register

12.7 In its comprehensive submission, the key change supported by the Marketing Association was to make compliance by marketers with its Do Not Call register mandatory. A mandatory Do Not Call register was also supported by OPC, the Advertising Standards Authority and a privacy lawyer.

12.8 The Marketing Association and the Advertising Standards Authority preferred the option of giving legislative backing to an industry-run scheme,[746] over the option of establishing a new government-run scheme.[747] This was on the basis of efficiency of resources and utilising the expertise of the Marketing Association.

12.9 There was also support in submissions for retaining the current voluntary Do Not Call register administered by the Marketing Association. One submitter suggested that the best option is to raise awareness of the voluntary scheme. Concerns about making the scheme mandatory were expressed by the Association of Market Research Organisations, NZ Post and Telecom. These concerns related to potential compliance costs for smaller operators and potential limits on calls to existing customers.

745 *Necessary and Desirable* at 76–78 (recommendation 25).

746 See for example the UK model, where the UK Direct Marketing Association administers the Telephone Preference System established under regulations and investigates complaints, and the South African model where the National Consumer Commission may recognise an industry registry as authoritative: Consumer Protection Act 2008 (South Africa), s 11(3); Direct Marketing Association of Southern Africa "The DMA Don't Contact Me Database Marketing Pre-emptive Block" < www.nationaloptout.co.za > .

747 See for example, the Australian Communications and Media Authority and the US Federal Trade Commission Do Not Call schemes, set up from scratch at considerable cost.

Electronic spam

12.10 Few submitters expressed concern with the control of electronic marketing messages under the Unsolicited Electronic Messages Act. The Marketing Association and OPC supported the current regime. OPC suggested that consideration could be given to moving the enforcement function under the Unsolicited Electronic Messages Act from the Department of Internal Affairs to OPC.

New developments

12.11 One development of note since the release of our issues paper, arising out of the review of the Credit Reporting Privacy Code, is the prohibition on the use or disclosure of credit information for direct marketing purposes.[748]

12.12 Another development is the release of the Article 29 Data Protection Working Party opinion on the adequacy of New Zealand's data protection legislation (that is, the Privacy Act) for purposes of the EU Data Protection Directive.[749] The Working Party found that New Zealand law does not fully comply with the EU direct marketing principle. This was not considered to be a major shortfall or an obstacle to the Working Party's finding that New Zealand ensures an adequate level of protection for purposes of the Directive. However, the Working Party expressed encouragement for New Zealand authorities to address weaknesses in the current legal framework and in particular for the Privacy Commissioner to continue her call for strengthening the law in relation to direct marketing.

12.13 Thirdly, the Marketing Association has informed us that is it working on a draft code of best practice for social media marketing.

Our response

12.14 We believe that there is currently a gap in the regulatory framework specifically in relation to telemarketing and that people should be able to access an efficient and user-friendly mechanism to address unwanted direct marketing approaches. It is currently difficult for people to unsubscribe from receiving unwanted telemarketing, unless they know about the Marketing Association Do Not Call scheme. As we noted in the issues paper, the Privacy Act enforcement framework is not particularly well suited to responding to consumer concerns about direct marketing.[750] We suggested that a more comprehensive, practical, cost-effective and consumer-friendly option might be needed.[751]

---

748 Office of the Privacy Commissioner *Amendment No 4 to the Credit Reporting Privacy Code 2004: Background Paper on Changes to Notified Amendment* (15 December 2010). This amendment to the Code commences on 1 October 2011 with respect to disclosure, and 1 April 2012 with respect to use. An amendment to the prohibition has been proposed to permit credit reporters to use direct marketing lists for pre-screening (that is, the removal of those who represent an adverse credit risk). See Office of the Privacy Commissioner *Proposed Amendment No 5 to the Credit Reporting Privacy Code 2004: Information Paper* (2011).

749 Article 29 Data Protection Working Party *Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand* (4 April 2011) 00665/11/EN WP 182.

750 Issues Paper at [15.15].

751 Ibid, at [15.16].

12.15 We have considered the option of introducing a new direct marketing principle in the Privacy Act (as in Australia) or amending the privacy principles to expressly articulate a right for people to opt out of receiving direct marketing. The problem with this approach is that it would require consumers to opt out on a case-by-case basis with each agency that directs marketing to them. This is likely to be inefficient and we think it would be frustrating and time-consuming for consumers to have to opt out on multiple occasions. It may also be more costly and time-consuming for marketers to implement one-off requests from consumers made at different times than to operate in accordance with a centrally-administered master list of consumer preferences.

12.16 Instead, we support the option of strengthening the current voluntary Do Not Call register administered by the Marketing Association by giving the scheme legislative backing so that it becomes mandatory for all marketers to observe recorded consumer preferences.[752] We agree that the most cost-effective and efficient option would be for the scheme to continue to be administered by the Marketing Association, backed up with enforcement powers from an appropriate regulatory body for cases which cannot be satisfactorily dealt with under the industry scheme. From overseas experience, it can be seen that a government-run scheme is likely to incur a high set-up cost.

12.17 However, we agree that the Privacy Act is not the best legislative vehicle to implement this measure. We have consulted the Ministry of Consumer Affairs to see if this is a measure that could be considered for implementation under consumer legislation. The Ministry has recently conducted a major review of consumer legislation, and as part of that review has considered the regulation of direct selling, including telemarketing.[753] The Ministry proposes new legislative provisions in the Fair Trading Act to replace the Door to Door Sales Act 1967. While noting the Marketing Association's voluntary Do Not Call register and the option raised in the Law Commission issues paper that compliance with the register could be made compulsory, the Ministry concluded that this requires further investigation.

12.18 Based on the support in submissions, especially from the industry self-regulatory body, we recommend that the Marketing Association's Do Not Call register be put on a statutory footing under the reformed consumer legislation and that the Ministry of Consumer Affairs initiate the necessary policy work to progress this initiative. In the meantime, we encourage the Ministry of Consumer Affairs and the Marketing Association to further publicise the current voluntary Do Not Call scheme to consumers.

12.19 Although we do not favour providing a case-by-case opt-out in the privacy principles as the primary mechanism for responding to telemarketing, we note that this may be a useful supplementary measure to our preferred option for a generic opt-out right under the Do Not Call register. For example, a case-by-case opt-out would allow people to opt out of any particular direct marketing that is not covered by the Do Not Call register. We think that the need for a case-by-case

752 See for example the South African model cited in n 746 above.

753 Ministry of Consumer Affairs *Consumer Law Reform Additional Paper: Regulation of Uninvited Direct Selling* (2010).

opt-out mechanism in the Privacy Act as a supplementary measure should be assessed in conjunction with implementation of a strengthened Do Not Call register.

RECOMMENDATION

R116 The Marketing Association's Do Not Call register should be put on a statutory footing under the reformed consumer legislation and the Ministry of Consumer Affairs should initiate the necessary policy work to progress this initiative.

Electronic spam

12.20 We do not support shifting the enforcement function under the Unsolicited Electronic Messages Act 2007 from the Department of Internal Affairs to the Privacy Commissioner. The focus of the Unsolicited Electronic Messages Act is on reducing unwanted electronic spam to promote confidence in the use of information and communication technologies for the benefit of electronic commerce.[754] We believe that the role of the Privacy Commissioner is most usefully reserved for issues where privacy is the central concern. We are also wary of recommending supplementary functions for the Privacy Commissioner who already has a sizeable number of functions and operates with a relatively small staff and budget.

Online behavioural targeting

12.21 In the direct marketing chapter of the issues paper we asked for comments about the appropriate regulatory response to issues raised by online behavioural targeting for advertising purposes. We respond to this topic in chapter 10.[755]

IDENTITY CRIME

12.22 We discussed the problem of identity crime in the issues paper, and outlined the applicable law. We noted a trend overseas towards enacting specific provisions targeting identity crime and asked whether any changes are needed to the Privacy Act or to other laws to better address this issue.[756]

Submissions

12.23 We received 12 submissions on this question. Submissions expressed support for:

- the Credit Reporting Privacy Code as a useful tool in responding to identity crime (three submitters);[757]
- new powers proposed for the Privacy Commissioner and new offences as being useful in responding to the issue: compliance notice and audit powers,[758]

754 See Unsolicited Electronic Messages Act 2007, s 3 (purpose section).

755 Ch 10 at [10.57]–[10.83].

756 Issues Paper at ch 17. See also Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, 2008) at [4.48]–[4.51].

757 Issues Paper at [17.34]–[17.37]; Office of the Privacy Commissioner *Amendment No 4 to the Credit Reporting Privacy Code 2004: Information Paper* (2010).

758 See R63–R64.

the proposed "pretexting" offence;[759] and the data breach notification requirement.[760]

- an amendment to principle 12 to encourage measures such as number truncation to control the public display of unique identifiers (three submitters);[761]
- new criminal offences (three submitters), although two further submitters suggested that further work is needed to scope the problem and assess the need for new offences; and
- other measures (the Police favouring measures to facilitate information sharing between agencies to allow identity crime to be investigated).

New developments

12.24 It is worth noting several relevant developments since the release of our issues paper.

12.25 First, the Credit Reporting Privacy Code has been revised to allow more comprehensive credit reporting. The Office of the Privacy Commissioner notes that one of the benefits is that this will provide a stronger base from which to detect identity theft and fraud, as the recording of accounts opened will enable the monitoring of unusual credit behaviour. The revised Code also includes additional safeguards, requiring credit reporters to be more transparent about the results of systematic reviews of their policies, procedures and controls and making them more accountable.[762]

12.26 Second, the Privacy Commissioner has proposed further changes to the Credit Reporting Privacy Code, including an amendment that would allow victims of identity fraud to seek suppression of their credit record, to prevent a fraudster from obtaining new lines of credit in their name.[763]

12.27 Third, the Identity Information Confirmation Bill 2010 has been introduced into Parliament. One of the purposes of the Bill is to facilitate the use of an electronic service, known as the Data Validation Service or DVS, that will allow agencies to confirm identity information about individuals recorded under the Births, Deaths, Marriages, and Relationships Registration Act 1995, the Passports Act 1992 and the Citizenship Act 1977, so as to contribute to the prevention of crime (particularly identity-related crime).[764] Use of the confirmation service would be subject to the agency or its intermediary obtaining the individual's consent to the identity check,[765] and being party to a confirmation agreement with the Registrar-General of Births, Deaths and Marriages and the Chief Executive of the Department of Internal Affairs.[766] The Privacy Commissioner must be

759 See R66(a).

760 See R67–R79.

761 Issues Paper at [17.57].

762 Office of the Privacy Commissioner, above n 757.

763 Office of the Privacy Commissioner *Proposed Amendment No 5 to the Credit Reporting Privacy Code 2004: Information Paper* (2011).

764 Identity Information Confirmation Bill 2010 (187–2), cl 4. See also Department of Internal Affairs *Identity Information Confirmation Bill: Regulatory Impact Statement* (2010).

765 Identity Information Confirmation Bill 2010 (187–2), cl 8(1)(a).

766 Identity Information Confirmation Bill 2010 (187–2), cl 8(1)(c).

consulted about the terms or conditions of confirmation agreements,[767] and the Commissioner may require these terms or conditions to be reviewed periodically.[768]

12.28 Fourth, the Department of Internal Affairs has developed guidance about detecting, preventing and responding to identity fraud.[769]

Our response

Amendment to principle 12

12.29 We support an amendment to principle 12 to encourage measures to control the publication of unique identifiers, as a response to the problem of identity crime. This amendment was first recommended by the Privacy Commissioner in a supplementary report to *Necessary and Desirable*.[770] One example of controlling the display of unique identifiers is the use of number truncation on credit card receipts.[771]

12.30 We discussed a number of options for amending principle 12 with OPC. Our preferred option is to add the following subclause, based on a reasonableness test:

> (5) An agency that discloses or displays an individual's unique identifier must take such steps (if any) as are reasonable to minimise the risk of misuse of the unique identifier.

What is anticipated is a graduated approach depending on the seriousness of the risk of misuse. The obligation to take reasonable steps will depend on the level of risk involved. What is reasonable may involve taking no steps at all, where any risk of misuse is low.

12.31 The proposed provision does not mention particular methods of protecting unique identifiers such as encryption, truncation or masking. In line with other privacy principles, the proposed provision is a statement of the desired outcome or objective (minimising the risk of misuse of the unique identifier), leaving a broad discretion to agencies as to how the objective is met. We recommend that Privacy Commissioner guidance be prepared that discusses the range of options available to agencies to minimise risk.[772] This guidance could also refer to relevant industry standards such as the standard developed by the Payment Card Industry Security Standards Council.

767 Identity Information Confirmation Bill 2010 (187–2), cls 12–13.

768 Identity Information Confirmation Bill 2010 (187–2), cl 14.

769 Department of Internal Affairs *Identity Assurance Framework: Good Practice Guide for Identity Fraud Control* (version 1.0, 2011).

770 *4th Supplement to Necessary and Desirable*, recommendation 28A.

771 Ibid, at 11. See also Issues Paper at [17.42] as to other potential measures.

772 See for example new sch 5 to the Credit Reporting Privacy Code, requiring hashing of driver licence numbers: Office of the Privacy Commissioner *Credit Reporting Privacy Code Amendment No. 4* (2010). The new schedule will come into force on 1 October 2011.

RECOMMENDATION

R117 Principle 12 should be amended to encourage measures to control the public display of unique identifiers, as a response to the problem of identity crime. The following subclause should be added to principle 12:

(5) An agency that discloses or displays an individual's unique identifier must take such steps (if any) as are reasonable to minimise the risk of misuse of the unique identifier.

RECOMMENDATION

R118 The Privacy Commissioner should produce guidance for agencies on the range of options available to address the risk of misuse of unique identifiers, with reference to any relevant industry standards.

Other measures

12.32 We do not make any recommendations about new criminal offences to specifically target identity crime. In this review we have focused in the main on whether changes should be made to the Privacy Act. We think that the question of additional offences in the Crimes Act addressing identity crime warrants its own review and needs to be looked at as a separate project.

12.33 We are not persuaded that the Privacy Act needs to specifically permit the disclosure of information about identity crimes to other agencies for the purpose of investigating and detecting identity crime, as suggested by the Police. We think that this is already adequately covered by the "maintenance of the law" exception to the disclosure principle. We discuss issues with this exception in chapter 9.

CULTURE AND PRIVACY

12.34 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.[773] We asked in the issues paper whether any special provision needed to be made for the needs and concerns of particular cultural groups in relation to privacy.

Māori

12.35 There is some evidence of distinct Māori perspectives on privacy,[774] and there are also precedents for making special provision in legislation for information of particular concern to Māori.[775] In the issues paper we invited submissions on whether there are any ways in which the Privacy Act or OPC could better

773 Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008) at 102–104 [*Privacy: Concepts and Issues*].

774 Ibid, at 104–108, 117–118; Khylee Quince "Maori Concepts and Privacy" in Steven Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (Brookers, Wellington, 2010) 27.

775 Issues Paper at 457.

provide for the needs of Māori. We also noted a number of issues that had been raised with us at a meeting with a group of Māori from a range of backgrounds that we held as part of this Review. The issues were:[776]

- tensions between individual-focused Western concepts of privacy and Māori concerns with collective interests;
- issues of trust and concerns by Māori that their information may be used in ways that are disempowering or derogatory, or that diminish mana;
- questions about the collection of personal information for iwi and hapū registers, and about governance of personal information held by tribal authorities; and
- concerns about control over online information about Māori, including whakapapa information.

12.36 We received few concrete suggestions in submissions for dealing with issues relating to Māori and privacy. A government department suggested a number of options:

- the development of guidance material dealing with issues that raise particular concerns for Māori;
- the establishment by OPC of an advisory group on issues of concern to Māori; and
- the development of a code of practice for the regulation of the handling of personal information in connection with iwi registers.

A lawyer also commented that guidelines in relation to Māori and privacy were needed. This submitter commented that there was "an inherent conflict between privacy, as a matter of individual autonomy, and concepts such as whanau and hapu, which rely on information sharing within a community". Such conflict, the submitter said, was particularly apparent in the health field, but could also come up in education and other areas. OPC said that its contacts with Māori had "not identified any bi-cultural issues that would need to be addressed by amendments to the Privacy Act". OPC considers that the Privacy Act:

> is a flexible piece of legislation that is well able to accommodate different cultural views about the nature and value of personal information and the desire to share, or limit the sharing, of personal information amongst a group.

OPC said that it is up to organisations to take advantage of the Act's flexibility in order to tailor their practices to meet individual and cultural preferences, but that monocultural attitudes may get in the way of doing so. OPC said that there may be scope for further work to assist agencies in this regard.

776 Ibid, at 458–460.

Other communities

12.37 We also asked in the issues paper whether there are any ways in which the needs and concerns of other cultural or religious groups in relation to privacy could be better met.

12.38 The Office of Ethnic Affairs submitted that, like all New Zealanders, individuals from ethnic communities wish to exercise control over their personal information and to keep some aspects of their lives private. However, they may differ from other New Zealanders in those aspects of their lives that they consider private, their levels of trust in government, their attitudes to the sharing of personal information, the likelihood of their lodging privacy complaints, and the most appropriate methods of communication with them. The Office submitted that:

> culturally appropriate mechanisms are needed to help people from different communities become aware of, and understand, their rights. The issue for ethnic communities is not so much the need for specific reference to ethnicity in privacy laws. Rather, it is more important that the relevant information is translated into major community languages and is readily accessible.

The Office's submission also referred to the need to consult ethnic communities about the handling of their personal information; to use ethnic media in raising awareness of privacy issues; and for the Privacy Commissioner to build relationships with ethnic community organisations and advocates.

Our response

12.39 One issue for consideration in relation to culture and privacy is whether the right to privacy can accommodate the collective interests of groups. We have already said in chapter 2 that we do not think that a group right to privacy can be recognised within the individual-focused framework of the Privacy Act. We do, however, think that making better provision in the Act for representative complaints, as recommended in chapter 6, could go some way towards recognising the privacy interests of groups. A representative complaint could, for example, be brought by a hapū or iwi in respect of a privacy breach affecting members of that group.

12.40 In addition, if Māori or other communities see certain types of information as belonging to groups rather than individuals, it may be possible to recognise this belief through areas of law other than privacy law, such as the developing field of indigenous intellectual property rights. Special legal mechanisms can be created in other legislation for certain types of sensitive information relating to Māori or other groups; for example, there are regulations providing for a National Kaitiaki Group to oversee the use of information about Māori women from the National Cervical Screening Register.[777]

777 Health (Cervical Screening (Kaitiaki)) Regulations 1995.

12.41 We note OPC's comments about the benefits of the flexible, open-textured nature of the Privacy Act, and encourage agencies to use that flexibility to apply the Act as much as possible in ways that are culturally appropriate. We also encourage OPC to further engage with Māori and ethnic communities to ensure that their particular privacy needs are being met. Such engagement could involve:

- sponsoring research into cultural beliefs about and attitudes to privacy;
- making information about the Privacy Act and privacy rights available in community languages;[778]
- producing guidance material about issues of concern to particular cultural communities (for example, guidance could be produced for Māori tribal authorities in relation to personal information on tribal registers); and
- producing guidance material for agencies about using the flexibility of the Privacy Act to accommodate cultural preferences.

12.42 In order to promote engagement by OPC with Māori and ethnic communities, we recommend an amendment to section 14 of the Act, which requires the Privacy Commissioner to have regard to certain matters. Section 14 should provide that, in exercising his or her functions and powers, the Privacy Commissioner must take account of the cultural diversity of New Zealand society, and of the needs and cultural perspectives of Māori in particular. Such a provision might be modelled on sections 11 and 13 of the Families Commission Act 2003. Section 11 of that Act is as follows:

> **Needs, values, and beliefs of particular groups**
>
> In the exercise and performance of its powers and functions, the Commission must have regard to the needs, values, and beliefs—
>
> (a) of Māori as tangata whenua:
>
> (b) of the Pacific Islands peoples of New Zealand:
>
> (c) of other ethnic and cultural groups in New Zealand.

The Families Commission is further required to "maintain mechanisms (for example, by appointing advisory committees or forming consultation forums) to ensure that there are at all times readily accessible to it the views" of the groups listed in section 11.[779] We think that this latter requirement to maintain appropriate mechanisms for engagement is a useful addition to a simple requirement to have regard to the needs, values and beliefs of particular groups.

RECOMMENDATION

R119 Section 14 should be amended to provide that, in exercising his or her functions, the Privacy Commissioner must take account of Māori needs and cultural perspectives, and of the cultural diversity of New Zealand society.

778 See, for example, the websites of the Broadcasting Standards Authority, the Human Rights Commission and the Health and Disability Commissioner, where information about people's rights is available in a range of languages.

779 Families Commission Act 2003, s 13(1). See also, for example, Law Commission Act 1985, s 5(2)(a): the Law Commission is required to "take into account te ao Maori (the Maori dimension)" and to "give consideration to the multicultural character of New Zealand society".

CHILDREN AND YOUNG PEOPLE

12.43 Children and young people are commonly seen as having particular vulnerabilities where privacy is concerned, because it is believed that they may not understand the consequences of misuse of their personal information as well as adults. Young people are also often said to be less concerned about their privacy than older people. At the same time, privacy laws are sometimes seen as an obstacle to the protection of vulnerable young people against abuse.

12.44 The question of young people's attitudes to privacy is a complex one.[780] It is often assumed that young people today, growing up in a world of constant connectivity via digital devices, have different attitudes to privacy from those of older generations. This may be true to some extent, but it is difficult to say at this point whether age-based differences in views of privacy are due to a generational shift in attitudes which will persist as today's young people grow older, or whether they relate more to particular phases in individuals' social and emotional development. It certainly does not appear to be the case that young people are uninterested in privacy, although their privacy concerns may be different from those of older people. According to American researcher danah boyd:[781]

> there is no radical shift in social norms because of social media. Teenagers care *deeply* about privacy. But they also want to participate in public life and they're trying to find ways to have both. Privacy is far from dead but it is definitely in a state of flux.

However, while young people do care about privacy, and many young people do take steps to protect their privacy, it does seem that young people are often unaware of some of the ways in which their information can be used by others. It is also important to realise that children and young people differ greatly among themselves: the privacy issues confronting young children are very different from those faced by teenagers, and young people's experiences will also vary depending on factors such as gender, class and ethnicity.

12.45 At present, there is only one provision in the Privacy Act that relates specifically to young people. Section 29(1)(d) provides that, in the case of an individual under the age of 16, an agency may refuse to disclose personal information requested under privacy principle 6 if the disclosure of that information would be contrary to that individual's interests. There are also provisions in the Health Information Privacy Code which have the effect of allowing parents and guardians of children under 16 to access their children's health information, unless there are good grounds for the agency to withhold that information.[782] While there have, at times, been perceptions that the Privacy Act prevents parents from finding out information about their children, such perceptions are often exaggerated or untrue. At the same time, it is true that the Act treats young people as individuals who are capable of exercising rights, and that parents will not always be entitled to have access to their children's personal information.

780 For further discussion see Law Commission *Privacy: Concepts and Issues*, above n 773, at 108–113; *For Your Information* at ch 67.

781 danah boyd "The Future of Privacy: How Privacy Norms can Inform Regulation" (speech to the International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 29 October 2010) available at < www.danah.org > .

782 See Issues Paper at 463.

Age of presumption of capacity

12.46 We asked in the issues paper whether the Privacy Act should provide more specifically for the age at which a child or young person should be treated as having capacity to exercise rights under the Act.[783] We noted that, currently, decisions about whether a young person has sufficient understanding and maturity to exercise rights under the Act are considered case-by-case. Providing expressly in the Act for an age of presumption of capacity could provide greater clarity for agencies. However, it could also be seen as inflexible and as preventing young people who are below the specified age from taking responsibility for their own personal information where they are capable of doing so. In addition, there could be difficulties with verifying age, particularly online. Another option which we mentioned in the issues paper would be to provide that an assessment of the young person's maturity should be carried out in order to determine whether he or she has capacity to exercise rights under the Act.

12.47 Submissions on this question put forward a range of views. More submitters supported than opposed the idea of prescribing in the Act an age at which young people are presumed to have capacity. YouthLaw said that having a specified age for presuming capacity in relation to accessing and correcting personal information would be useful. They said that it can be difficult for children and young people to access their personal information, or to have their personal information corrected, on their own behalf, in the absence of a clear provision in the Act stating that they are entitled to do so. YouthLaw said the age for presumption of capacity in relation to access and correction should be 16 at the most, and that the Act should expressly provide that agencies must still carry out an assessment of capacity in relation to young people below the prescribed age who seek to exercise these rights. The Ministry of Social Development submitted that the Ministry (and particularly Child, Youth & Family) frequently experiences uncertainty about when a child or young person can or cannot exercise rights such as accessing personal information or authorising disclosure of personal information. The Ministry said that this issue is particularly difficult when children and parents have different views, and clarification in legislation would be welcome. On the other hand, both OPC and the Children's Commissioner said that the Act should not provide for an age of presumption of capacity. The Children's Commissioner commented that, if the Act were to prescribe an age of presumptive capacity, there is a danger that children under that age will be presumed not to have capacity. Such an approach, in the Commissioner's view, is inconsistent with the ideas of children's rights and of evolving capacities. The Commissioner stated that children are entitled to have a say in the use of their personal information, with the guidance of their parents, and that due consideration should be given to a child's views according to the child's age and maturity.

783 Ibid, at 466–467.

12.48 We think that, in considering this question, it is useful to be specific about the rights that an age of presumption of capacity might apply to. In our view, there are three matters in respect of which the Act could provide for such an age:

- bringing a complaint;
- making an access or correction request; and
- authorising the collection, use or disclosure of an individual's own personal information.

12.49 We do not think it would be helpful to provide for the age at which a young person can bring a complaint under the Act. At present, section 67 provides that "any person" can make a complaint to the Privacy Commissioner. The complainant does not need to be the individual who was affected by an alleged interference with privacy. Thus, a complaint could be brought on behalf of a child by a parent or guardian, but equally a child or young person is not prevented from making a complaint on his or her own behalf. We think this flexibility is appropriate, and that no more specific provision is needed. We can see no reason why a complaint made by a child or young person should not be considered by the Commissioner, and we note that the Commissioner has quite broad discretion under section 71 not to investigate, or to discontinue an investigation.

12.50 We recommend that the Act should not provide for an age at which an individual can make an access or correction request. We believe that the Act currently allows young people to make access and correction requests, since there is nothing in the Act preventing them from doing so. This is appropriate, in our view. There will, in some circumstances, be good reasons why an agency should withhold personal information that a young person has requested under principle 6. However, the withholding of information relating to individuals under the age of 16 is already provided for by section 29(1)(d), and we can see no reason to change this provision. It may be appropriate, in deciding whether access should be refused under section 29(1)(d), to consult the young person's parents or guardians, but parents or guardians do not have a right of veto over an application by a young person for access to his or her own information.

12.51 We have found the question of whether the Act should provide for an age at which an individual can provide authorisation to be particularly difficult. Such a provision would relate to the authorisation exceptions to the collection, use and disclosure principles. If an agency obtains the authorisation of the individual concerned, it can collect personal information from someone other than that individual, and can use or disclose that individual's personal information for purposes other than those for which the information was obtained. In theory, it would seem desirable to specify in the Act an age at which an individual is presumed to be able to provide authorisation on his or her own behalf. It is important that those authorising the collection, use or disclosure of their information should understand fully what it is that they are agreeing to, and very young individuals are unlikely to be able to provide properly-informed consent in relation to the handling of their personal information. Providing for an age at which individuals are presumed to have capacity for the purposes of the authorisation exceptions could be seen as providing greater protections for children, and greater clarity for agencies.

12.52 Despite these arguments in favour of specifying an age of presumption of capacity in relation to authorisation, we think that the difficulties of doing so outweigh the benefits. One difficulty concerns verification of age. If the Act is to provide for an age at which individuals have capacity to authorise on their own behalf, does this mean that agencies must take steps to verify an individual's age? If so, how is this to be done, particularly online? We think that the difficulties of providing adequately for such matters in statute are almost insurmountable in an age when so much interaction between individuals and agencies takes place online. A second difficulty concerns authorisation by parents and guardians on their children's behalf. If the Act were to state that young people above a certain age can provide authorisation on their own behalf, this immediately raises the question of whether parents and guardians should be able to authorise on behalf of children below the specified age. It must be the case that parents and guardians can authorise on behalf of their children in some cases, particularly where those children are very young. But again, we think that providing expressly for this in statute is fraught with difficulties. What about parents who have only rights of contact with their children, not day-to-day care? What if parents disagree with each other, or with the clearly-expressed views of the child concerned? What if authorisation provided by a parent or guardian is contrary to the best interests of the child?

12.53 Given such difficulties, we recommend that the Act should make no provision for the age at which individuals can provide authorisation on their own behalf, or for authorisation by parents or guardians on a child's behalf. These matters should be considered case-by-case, as at present, using the Act's inherent flexibility. We understand from OPC that these issues do not in fact arise frequently, or cause significant problems, and therefore we think that it is better to leave matters as they are.

Should the Act contain additional protections for young people?

12.54 In the issues paper we asked whether any new protections for young people were needed in the Act, and specifically whether any particular protections were needed in relation to online privacy or direct marketing.[784] The apparent willingness of young people to disclose information about themselves online is often seen as putting them at risk from threats such as identity crime and sexual exploitation, and as creating problems for their future lives when information that they have posted about themselves online may prove embarrassing or may harm their employment, educational or other prospects. Commercialisation of children's online space has also been raised as a concern, with sites targeted at children sometimes collecting information for use in marketing in ways that children are unaware of.[785] It has been argued that

784 Issues Paper at 464–466.

785 A survey of websites by the *Wall Street Journal* in the United States found that sites popular with children and teenagers placed 30 per cent more pieces of tracking technology (such as "cookies") on the computers of those using them than did sites aimed primarily at adults. Not all of these tools were intended to track or monitor the online activity of individuals: some simply remember where users are up to when they pause a game, for example. Steve Stecklow "On the Web, Children Face Intensive Tracking" *Wall Street Journal* (17 September 2010) < online.wsj.com > .

children are less able than adults to distinguish advertising from other content, and that the internet allows advertisers to target children in an environment where they are often unsupervised.

12.55 A number of submissions supported educational measures to address concerns about young people's privacy. Both OPC and YouthLaw saw education as a necessary, though perhaps not sufficient response to such concerns. YouthLaw commented that often young people will disclose their personal information not because they are untroubled about releasing this information but because they are unaware of the extent to which it can be used. They considered that education needed to be combined with legal requirements on agencies, to ensure that young people can make good decisions on the use of their personal information but are also protected from those seeking to misuse that information. OPC said that they have prioritised awareness-raising and educational work with young people in the recent past. This work has included setting up a youth advisory group and developing educational resources for young people. In addition to education, OPC and YouthLaw both supported the further exploration of statutory provisions that would impose heightened obligations on websites targeting children. OPC also thought that general reforms to the Privacy Act, such as the creation of a power for the Privacy Commissioner to issue compliance notices, could help to deal with issues about young people's privacy. Another submission suggested that marketing to children could be dealt with through a voluntary code.

12.56 While we received relatively few submissions on privacy issues relating to children and young people, we believe that these are issues of significant public concern. The most recent public opinion survey carried out for the Privacy Commissioner found that 88 per cent of respondents were concerned about "the information children put on the internet about themselves".[786] There is also a great deal of coverage in the media of online privacy and safety issues relating to young people. Options for addressing these concerns include:

- education;
- voluntary industry codes; and
- legislation.

12.57 We strongly support action to educate and raise awareness among young people about privacy issues. We welcome the fact that there are a range of existing initiatives aimed at educating young people and their parents about online privacy and safety, and at empowering young people to protect themselves online. Such initiatives include:

- the establishment by OPC of a youth advisory group, and the development of privacy resources for young people;[787]
- the work of NetSafe, a non-profit organisation which is involved in education and promotion of safe and responsible use of cyberspace, and which produces information aimed at young people and their parents;[788]

786 Privacy Commissioner/UMR Research *Individual Privacy and Personal Information: UMR Omnibus Results March 2010* at 19–20. Seventy-two per cent of respondents were "very concerned".

787 < http://privacy.org.nz/youth > .

788 < www.netsafe.org.nz > .

- Hector's World, a website developed in New Zealand by NetSafe, which provides educational material about online safety and privacy aimed at young children;[789] and
- information about child safety online provided by the Department of Internal Affairs.[790]

We encourage these and other agencies to continue their efforts in this area.

12.58 There was little call in submissions for legislative change to protect young people's privacy. However, OPC and YouthLaw did see a case for increased legislative protection in relation to children's privacy online, including requirements to demonstrate informed consent from young people or their parents for the collection of young people's information. An example of such legislation, which we cited in the issues paper and which was referred to by OPC and YouthLaw, is the Children's Online Privacy Protection Act of 1998 (COPPA) in the United States.[791] COPPA applies to websites directed at children under the age of 13 and to other websites that have "actual knowledge" that they are collecting information from children under 13. Such websites are required to obtain parental consent before collecting personal information from children under 13, and to post electronic privacy notices explaining their collection and use of children's personal information. COPPA has been criticised on a number of grounds, including that it is easy for children to lie about their age in order to access websites aimed at an older audience, that it is difficult to verify parental consent, and that 13 is an arbitrary age limit. On the other hand, some United States privacy advocates see it as a useful check on the collection of personal information from children (particularly in the absence of a generally-applicable privacy law in the United States), although they say it needs to be strengthened.[792]

An amendment to principle 4

12.59 We do not see the COPPA model as a useful one for New Zealand. The difficulties of verifying age and consent online are so great that we do not think it is possible to provide for such verification in legislation. Furthermore, New Zealand is not in the same position as the United States: we have an effective privacy law of general application, which protects children and young people just as much as adults. However, we do think that agencies collecting information from children, whether online or otherwise, should take particular care on account of children's vulnerability. This vulnerability results in large part from the fact that children and young people are often less able than adults to understand the possible consequences of the collection of their personal information. Young children in particular are also likely to be less able to protect themselves against the collection of personal information by surreptitious or deceptive means.

789 < www.hectorsworld.org > .

790 Department of Internal Affairs "Child Safety Online" < www.dia.govt.nz > .

791 91 USC § 6501–6506.

792 Alice E Marwick, Diego Murgia Diaz and John Palfrey *Youth, Privacy and Reputation: Literature Review* (Berkman Center for Internet & Society, Harvard University, Research Publication 2010–5) at 38–41; danah boyd "How COPPA Fails Parents, Educators, Youth" (10 June 2010) Apophenia < www.zephoria.org > ; Courtenay Banks "Understanding the Children's Online Privacy Protection Act" *Wall Street Journal* Digits blog (17 September 2010) < blogs.wsj.com/digits > ; Matt Richtel and Miguel Helft "Facebook Users who are Under Age Raise Concerns" *New York Times* (11 March 2011) < www.nytimes.com > .

12.60 Privacy principle 4 provides protection against the collection of personal information by means that are unfair in the particular circumstances, or that intrude unreasonably on an individual's personal affairs. This principle is particularly relevant where information is being collected from children, and we think that the principle should more clearly signal that age is a relevant factor in relation to unfairness or intrusiveness of collection practices. We therefore recommend that privacy principle 4 should be amended by adding a new subclause. This subclause should provide that, in considering whether the collection of personal information is unfair or unreasonably intrusive for the purposes of principle 4(b), the age of the individual concerned must be taken into account.

12.61 We have deliberately referred in our recommendation to "age" rather than "youth", since we think that in some circumstances it will be relevant to take into account the fact that the individual concerned is elderly. Although we have focused in this discussion on children and young people, we think that elderly people may be equally vulnerable to unfair collection of personal information. Reasons for this vulnerability include declining cognitive faculties, susceptibility to pressure from marketers or others, and lack of familiarity with digital technologies. We have considered whether the new subclause should be broadened still further, to require agencies to take account of the "vulnerability" of the individual concerned. However, vulnerability is a much more subjective factor than age, and we think that referring to vulnerability in principle 4 would create too much uncertainty.

12.62 We further recommend that the Privacy Commissioner should develop guidance with respect to the new provision in principle 4, to explain to agencies the steps they should take to avoid unfair or unreasonably intrusive collection of information from children, young people and the elderly.

RECOMMENDATION

R120 Principle 4 should be amended to provide that, in considering whether the collection of personal information is unfair or unreasonably intrusive for the purposes of principle 4(b), the age of the individual concerned must be taken into account. The Privacy Commissioner should develop guidance material with respect to this new provision.

Marketing to children and young people

12.63 We think that industry self-regulation is the best way of dealing with issues concerning marketing to children. Self-regulation is in line with established practice for the advertising and marketing industries in New Zealand. While concerns about marketing to children have a significant privacy component, they also go well beyond privacy. The general field of marketing to children is beyond the scope of this report, but we can comment here on the adequacy of privacy protection in existing regulation of marketing to children. The Advertising Standards Authority (ASA) has a Code for Advertising to Children, which is concerned with children under the age of 14. The Code states that:[793]

> Extreme care should be taken in requesting or recording the names, addresses and other personal details of children to ensure children's privacy rights are fully protected and the information is not used in an inappropriate manner.

The Marketing Association's Code of Practice for Direct Marketing in New Zealand deals only briefly with marketing to children, and does not deal specifically with children's privacy issues.[794] The Marketing Association does not have a separate code of practice specifically addressing marketing to children. Both the ASA's and the Marketing Association's codes have been reviewed relatively recently. Nonetheless, we think it would be desirable for these organisations, and other relevant industry bodies, to consider whether existing codes provide adequate coverage of privacy issues relating to marketing to children. We suggest that the codes referred to above could deal more fully with children's privacy. The Marketing Association could also consider developing a separate code for marketing to children, giving particular attention to online marketing.[795] We note that both of the codes discussed above relate only to children under the age of 14, and we suggest that particular care should also be taken with marketing to young people aged 14 and over.[796]

RECOMMENDATION

R121 The Advertising Standards Authority, the Marketing Association and any other relevant industry bodies should review the adequacy of privacy protection in existing codes that regulate marketing to children.

793 Advertising Standards Authority *Code for Advertising to Children* (August 2010) principle 2(i). The Code also draws attention to privacy principle 3 of the Privacy Act.

794 Marketing Association *Code of Practice for Direct Marketing in New Zealand* (reviewed October 2009) principle 1(c) (marketers must abide by the ASA's Code for Advertising to Children); principle 4(a) (marketers must not knowingly take orders from children under the age of 14 without parental approval).

795 See the discussion of the regulation of marketing to children in the UK in Jillian Pitt *A Tangled Web: Marketing to Children* (Consumer Focus, London, 2010).

796 A comparison can be drawn here with the ASA's codes on food advertising. While the ASA has a special Children's Code for Advertising Food, which applies only to children younger than 14, its main Code for Advertising Food notes that advertisers are "required to exercise a particular duty of care for food advertisements directed at young people aged 14 to 17 years of age". Advertising Standards Authority *Code for Advertising Food* (August 2010) introduction.

Best interests of the child

12.64 The Children's Commissioner submitted that the Privacy Act should include a "best interests of the child" provision "to ensure the proper balance is struck between competing interests when children are involved." Article 3(1) of the United Nations Convention on the Rights of the Child, which has been ratified by New Zealand, states that:

> In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.

There are precedents in New Zealand legislation for referring expressly to the best interests of the child.[797] The best interests of the child are also referred to in the privacy principles of the Broadcasting Standards Authority.[798]

12.65 We do not recommend the inclusion of a general "best interests of the child" provision in the Privacy Act. We are not convinced that such a provision would help to resolve tensions between privacy and child welfare, where such tensions exist. If it is considered that privacy protections are inhibiting the disclosure of personal information that is necessary for the protection of children's welfare, then specific provisions can authorise or require the sharing of personal information for child welfare purposes.[799] The existing exceptions to the privacy principles are also flexible enough to be used to protect children's interests. Our recommendation in chapter 3 to remove the word "imminent" from the health and safety exceptions to the use and disclosure principles should allow agencies greater scope in situations where children face serious threats to health and safety but the danger is not immediate. Furthermore, New Zealand's obligations under international human rights instruments are relevant to the interpretation of a statute even if the statute does not expressly refer to those obligations. Thus, so long as the "best interests of the child" principle is not inconsistent with the clear wording of the Privacy Act, decision-makers should take that principle into account in applying the Act, where it is relevant to do so.

12.66 Nonetheless, we think there is one place in the Act where reference to the best interests of the child can readily be incorporated in a way that signals the need to take such interests into account. Section 14(b) provides that, in performing his or her functions and exercising his or her powers, the Privacy Commissioner shall "take account of international obligations accepted by New Zealand, including those concerning the international technology of communications". We recommend that reference should also be made in this section to international obligations concerning the rights and best interests of the child.

797 See particularly Care of Children Act 2004, ss 4–5.

798 Broadcasting Standards Authority, privacy principle 6. The BSA principles state that, if a broadcast breaches a child's privacy, the broadcaster must be satisfied that the broadcast is in the child's best interests, even if consent has been obtained. A child's guardian can consent to the broadcast of information about a child under the BSA principles.

799 See our discussion of information sharing in appendix 1.

RECOMMENDATION

R122 Section 14(b) should be amended to refer to New Zealand's international obligations concerning the rights and best interests of the child.

OTHER PEOPLE WITH PARTICULAR NEEDS

12.67 We asked in the issues paper whether the Privacy Act should make particular provision for adults with reduced capacity.[800] We said that some individuals have a reduced capacity to act on their own behalf, particularly when it comes to giving or withholding authorisation to the collection, use or disclosure of their personal information. Individuals with reduced capacity could include those with intellectual disabilities, mental illnesses or dementia. There is a presumption in both common law and statute that all adults have capacity until the contrary is proved.[801] However, New Zealand law also recognises the need in some circumstances for another person to make decisions on behalf of a person with a temporary or permanent incapacity. We asked whether the Privacy Act should expressly provide for a person acting under legal authority to act on behalf of another who is affected by incapacity, and whether the Act should make any special provision for people with reduced capacity where such individuals do not have a legally-recognised representative. We noted that there are provisions in the Health Information Privacy Code relating to disclosure of health information to an individual's representative in circumstances where the individual is unable to give consent or to exercise his or her rights.

12.68 Several submitters supported the idea of providing greater clarity with respect to the exercise of rights under the Privacy Act in relation to adults with reduced capacity. The Ministry of Health said that it would be better to deal with this issue through guidance material, and also suggested that the general law in the area of decision-making on behalf of people with temporary or permanent incapacity is in need of review. The Human Rights Commission and IHC argued strongly against any provision based on substituted decision-making. Both organisations drew our attention to the United Nations Convention on the Rights of Persons with Disabilities, ratified by New Zealand in 2008, which allows for decision-making on behalf of others only as a last resort.[802] The Human Rights Commission opposed specific provisions for people with reduced capacity, and said that the common law presumption of capacity should prevail except where a welfare or property guardian has been appointed under the Protection of Personal and Property Rights Act 1988, or an advance directive exists. IHC, which works in the area of intellectual disability, said that, rather than talking about people with reduced capacity, it is better to refer to people who need support to exercise their capacity. What is needed, IHC said, is support for people with intellectual disabilities to make their own decisions, rather than the substitution of decision-making by others on behalf of people with intellectual disabilities:

800 Issues Paper at 467–469.

801 Protection of Personal and Property Rights Act 1988, s 5.

802 See particularly Convention on the Rights of Persons with Disabilities, art 12.

> What needs to be recognised for this review is the ability for people with intellectual and other disabilities to choose support persons, including social interpreters, to assist them directly to exercise their rights under the Privacy Act. They also need to be able to choose who acts for them. In addition, agencies have responsibilities to provide for the support needed to exercise their rights.

IHC supported the provision of guidance by the Privacy Commissioner, based on a supported decision-making model. IHC also proposed the establishment of a working group, including disabled people and their organisations, to consider and address capacity issues.

12.69 In light particularly of the submissions from the Human Rights Commission and IHC, we recommend that the Privacy Act should make no specific provision for issues of legal capacity. This approach is consistent with that taken by the Australian Law Reform Commission.[803] Where a person is empowered under the Protection of Personal and Property Rights Act or other law to act on behalf of another, we do not think it is necessary for the Privacy Act to expressly recognise such legal authority. A couple of submitters said that the legal framework governing decision-making on behalf of people with incapacity is itself in need of review, but this matter is outside the scope of our present review. Where an individual does not have a legally-authorised representative, we do not think any special provision in the Act is warranted. We endorse the supported decision-making model put forward by the Human Rights Commission and IHC, and IHC's proposal for the establishment of a working group to consider capacity issues. Such a working group should be convened by OPC, but should be representative of individuals and organisations with experience of intellectual disability and other matters relating to capacity. The working group should produce guidance on issues of capacity and supported decision-making under the Privacy Act. It may be that several pieces of guidance would be necessary, as the issues for people with intellectual disability will be quite different from those for people with mental illness, for example. We note that OPC and the Mental Health Commission have already collaborated to produce guidance material for health practitioners on mental health information.[804]

12.70 A related question which we mentioned but did not explore in the issues paper is whether anything needs to be done to address privacy issues for people with physical disabilities. In its submission, the Human Rights Commission urged us to actively engage with the disability community about their specific needs, and IHC said that, like people with intellectual disabilities, people with physical disabilities may need support to exercise their rights under the Act. We have not been in a position to consult further on the needs of people with disabilities, but we support further exploration of issues concerning disability and privacy. It may be that the working group discussed in the previous paragraph could also consider issues for people with physical disabilities, but it could also be that it is more appropriate to explore these issues separately. We recommend that either OPC or another appropriate body (such as the Human Rights Commission or the Office of Disability Issues within the Ministry of Social Development) should facilitate work in this area, in partnership with disabled people's organisations.

803 *For Your Information* at 2344–2361.

804 Mental Health Commission and Office of the Privacy Commissioner *Guidance Material for Health Practitioners on Mental Health Information* (2009).

It is worth noting that the Health Information Privacy Code (HIPC) applies to information about disabilities and to providers of disability services. In its submission, IHC questioned the appropriateness of including disability in the HIPC, and said that disabled people prefer that health services and disability services are recognised as separate, with different contexts and imperatives.

RECOMMENDATION

R123 The Office of the Privacy Commissioner should convene a working group to consider issues of capacity under the Privacy Act, and to develop guidance material based, as much as possible, on supported decision-making.

RECOMMENDATION

R124 Further work should be undertaken to explore issues of privacy and disability. This work should be facilitated by the Office of the Privacy Commissioner or another appropriate body, and should be carried out in partnership with disabled people's organisations.

WORKPLACE PRIVACY

12.71 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 numbers, salary information, CVs, performance reviews and medical information. Some of this information is very sensitive.

12.72 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). Again, new technologies are increasing the potential for employers to gather more information about employees.

12.73 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.

12.74 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, confidence and good faith. The requirements of the Health and Safety in Employment Act 1992 may sometimes justify a lesser degree of privacy in order to ensure safety (for example, monitoring). Other statutes, including our criminal legislation,[805] obviously apply in the workplace as much as anywhere else. Discriminatory treatment by employers is covered by both the Employment Relations Act 2000

805 In particular, the criminal law covering surveillance: see Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at 12–13 [*Penalties and Remedies*].

and the 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.

12.75 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.

12.76 In the issues paper we put forward some potential options for the law on workplace privacy.[806] They included the status quo; specific workplace privacy legislation; codes of practice, whether under the Privacy Act or the Employment Relations Act; and guidance by the Privacy Commissioner. We surveyed overseas developments, noting in particular the Victorian Law Reform Commission's proposal (as yet not acted on) for a Workplace Privacy Bill.

12.77 We did not receive many submissions on this aspect of the issues paper. The submission from the New Zealand Council of Trade Unions expressed concern at the ease with which employers seem to be able to justify non-compliance with the Privacy Act. They emphasised in particular requests for access to personal information which are effectively coerced (a matter we deal with in chapter 3) and requirements to disclose use of medicines or underlying medical conditions. They also outlined a number of matters relating to surveillance which fall more within the scope of stage 3 of our project.

12.78 There was no call in any of the submissions for separate workplace privacy legislation. Two submitters thought no action was required, while four indicated that if anything were to be done a code of practice was the most appropriate vehicle. (As well as the Privacy Act, the Employment Relations Act 2000, section 100A, confers power to make codes.) NZCTU put forward the interesting suggestion that there should be model draft clauses for employment agreements on privacy processes, and that information about workplace privacy should be more readily accessible.

12.79 The recommendations we have made earlier in this report for amendments to the Privacy Act will apply as much to the workplace as to any other context. They will help to address some of the concerns expressed in the submissions about workplace privacy. However, we do not detect sufficient support for us to make any firm recommendations for special workplace privacy legislation at this time. We reached a similar conclusion, in relation to workplace surveillance, in our report on stage 3 of this Review.[807] But employment relations are a matter of the greatest importance, and we believe that the issue of workplace privacy should be kept under close review, particularly in the light of advances in technology. If action becomes necessary, a code of practice made under either the Privacy Act or the Employment Relations Act would seem the best option.

806 Issues Paper at [19.24]–[19.27].

807 Law Commission *Penalties and Remedies*, above n 805, at 86–87.

HEALTH INFORMATION

12.80 Information is vital to health care. In the course of medical treatment, a wide variety of personal information might be required and 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.

12.81 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 the benefit of patients and the wider community. The future health of citizens also depends on medical research. Researchers need access to case information.

12.82 While disclosure of health information to *appropriate* persons is important, beyond this privacy and confidentiality are especially important in health. Maintaining confidentiality is essential to the doctor/patient relationship, to ensure patient trust. Medical codes of ethics place strong emphasis on confidentiality. Without an assurance that their personal health information will be protected, people might not seek help when they need it. Such an assurance 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.

12.83 Thus, a difficult balance must be struck between, on the one hand, keeping personal information confidential, and on the other, getting the right information to the right person when it is needed. It is important that patients are aware of how their information will be used.

12.84 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 could be more vulnerable in the absence of strict controls. Developments in genetic testing also raise difficult privacy issues.

12.85 The law governing health information and privacy is mainly made up of the Privacy Act and HIPC, together with the Health Act 1956.[808] There are further provisions scattered across a number of other statutes.[809] This framework is not very coherent.

808 Issues Paper at [19.8]–[19.14].

809 Ibid, at [19.6], n 1615.

12.86 In this report we have already made some recommendations with implications for health information. We note in particular the modification to the health and safety exception to principles 10 and 11, and the proposed new health and safety exceptions to principles 2 and 6.[810]

12.87 However, given the sensitivity, complexity and importance of healthcare, the Law Commission put the suggestion in the issues paper that the whole subject of health information needs separate review, with a view to enacting separate comprehensive legislation.[811] That legislation should set 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.

Such a review would extend to such matters as human tissue samples, which we discuss in another context elsewhere in this report.[812]

12.88 What we have in mind goes beyond privacy, and would cover how health information as a whole is handled. The Ministry of Health must obviously be involved in such a review: they have already done much work on specific issues, including human tissue samples. The review would also need to take account of the significant body of work on use and governance of health information currently going on under the leadership of the National Health Information Technology Board.[813]

12.89 There was substantial support in submissions for a comprehensive separate review. The supportive submissions made some significant points:

- Business NZ noted a need for greater clarity about the relationship between the Privacy Act and the Health and Safety in Employment Act.
- IHC questioned the appropriateness of disability support services being included in the HIPC: it is based, they said, on a former medical model of disability.
- The New Zealand Law Society said that consideration should be given to compulsory privacy impact assessments (PIAs) for medical databases (as in Canada and the United States).

12.90 Not all submitters supported comprehensive new health legislation, however. The Women's Health Action Trust would prefer to see increased resources put into enhancement of the HIPC as technology advances. They also emphasised the importance of consumers' right to consent, particularly in the context of medical research. OPC wished to distinguish between a health *privacy* statute and a health *information* statute. While a new health information statute may be desirable, and could be a place where the legitimacy of information collections

810 See ch 3, R12, R22 and R31.

811 Issues Paper at [19.16].

812 See ch 2.

813 < www.ithealthboard.health.nz > .

(such as screening programmes) can be established along with special rules that may support or prevail over routine privacy expectations, OPC does not accept that there is a case for a special health privacy statute, which would result in further fragmentation of privacy law.

12.91 Given the complexity and sensitivity of the area, we confirm our view as expressed in the issues paper that it merits separate review. The Ministry of Health should be centrally involved in such a review.

RECOMMENDATION

R125 The Government should conduct a review of the handling of health information, with a view to enacting separate comprehensive legislation.

PRIVACY OFFICERS

12.92 Section 23 of the Privacy Act provides that:

> It shall be the responsibility of each agency to ensure that there are, within that agency, 1 or more individuals whose responsibilities include—
>
> (a) the encouragement of compliance, by the agency, with the information privacy principles:
>
> (b) dealing with requests made to the agency pursuant to this Act:
>
> (c) working with the Commissioner in relation to investigations conducted pursuant to Part 8 in relation to the agency:
>
> (d) otherwise ensuring compliance by the agency with the provisions of this Act.

It is notable that there is no penalty for failure to appoint a privacy officer.

12.93 OPC's website says that a privacy officer:[814]

- is familiar with the privacy principles in the Privacy Act
- is familiar with any other legislation governing what the agency can and cannot do with personal information
- deals with any complaints from the agency's clients about possible breaches of privacy
- trains other staff at the agency to deal with privacy properly
- advises managers on how to ensure the agency's business practices comply with privacy requirements
- advises managers on the privacy impacts (if any) of changes to the agency's business practices
- advises managers if improving privacy practices might improve the business
- deals with requests for access to personal information, or correction of personal information
- acts as a liaison person for the agency with the Privacy Commissioner. (This is particularly important if the Privacy Commissioner is investigating whether the agency has breached privacy).

814 Office of the Privacy Commissioner "Privacy Officers" < http://privacy.org.nz/privacy-officers > .

12.94 We did not ask any questions about privacy officers in our issues paper, and there was very little mention of privacy officers in submissions, with the exception of the submission from OPC. OPC noted that the obligation to appoint privacy officers was a New Zealand innovation which has since been adopted elsewhere. OPC said that the privacy officer mechanism is a valuable part of the Act, although it is inconsistently complied with.

12.95 In its submission, OPC proposed the following reforms in relation to privacy officers:

- allowing agencies to appoint external persons as privacy officers;
- empowering the Privacy Commissioner to require agencies to appoint privacy officers;
- providing privacy officers with statutory protection against victimisation;
- imposing additional responsibilities on privacy officers in larger agencies;
- identifying public policy roles that should be played by privacy officers in government departments; and
- appointing a whole-of-government Chief Privacy Officer for the state sector.

12.96 We endorse OPC's comments about the value of the privacy officer mechanism when it is used well: that is, when the privacy officer has the necessary skills and when the agency provides the privacy officer with the support necessary to do his or her job. Having someone within an agency who is charged with ensuring that the agency complies with the Act's requirements is an integral part of the Act's light-handed approach to regulation, which relies in the first instance on agencies to ensure their own compliance. We also endorse the observations of the Privacy Commissioner in *Necessary and Desirable* about the importance of agencies offering support and training for their privacy officers, and about the value of privacy officers networking to share their experiences.[815] On the latter point, a Privacy Officers' Round Table was established in 2005, on the initiative of the Privacy Commissioner, and meets regularly.[816]

12.97 Our responses to OPC's reform proposals are as follows:

- We agree with the recommendation made by the Privacy Commissioner in *Necessary and Desirable* that agencies should be allowed to appoint a privacy officer from outside the agency.[817] This would involve deleting the words "within that agency" from section 23. For smaller agencies, it may make more sense to pay an outside consultant to undertake the privacy officer role, rather than appointing someone from within the agency.
- We have recommended in chapter 6 that the Privacy Commissioner should be given a power to issue compliance notices. This power would allow the Privacy Commissioner to require an agency to comply with section 23 by appointing a privacy officer.

815 *Necessary and Desirable* at 138–139.

816 "PORT – the Privacy Officers' Round Table" < http://privacy.org.nz/port-the-privacy-officers-round-table > .

817 *Necessary and Desirable* at 137–138.

- We considered in chapter 3 whether the Privacy Act should include a general anti-victimisation provision, but decided that such a provision is not needed. As we said in chapter 3, if a privacy officer is disadvantaged or victimised for carrying out his or her duties, there will be remedies available in employment law.
- We do not think that the Privacy Act needs to provide for additional duties or responsibilities for larger agencies or for government departments. Section 23 spells out the general role of the privacy officer adequately, in our view. Additional specificity can be provided in guidance material from OPC, the State Services Commission (for the public sector), or other appropriate bodies.[818]
- We are not opposed to the idea of a Chief Privacy Officer for the state sector, but we are not inclined to recommend such an appointment. We do have some concerns about differentiating the respective roles of the Chief Privacy Officer and the Privacy Commissioner, and about the potential for agencies to receive conflicting advice from these two officials.

RECOMMENDATION

R126 Section 23 should be amended to allow agencies to appoint a privacy officer from outside the agency.

818 For an overseas example of such guidelines see Network of Data Protection Officers of the EU Institutions and Bodies *Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2001* (2010).

Appendices

Appendices

Our issues paper on the Review of the Privacy Act contains chapters on **information sharing** and **information matching**. The first of these is about the ability of government agencies to share personal information about individuals. Such sharing may be with a view to providing better and more efficient service for individuals and families. It may be with a view to detecting wrongdoing. It may indeed be for any of a large number of purposes. But such arrangements do have significant implications for the privacy of the individual. This question was of considerable interest to the Government, and the Minister Responsible for the Law Commission asked the Commission to publish its conclusions on information sharing in advance of our final report on the review of the Act. We did so on 29 March 2011 in the form of a Ministerial Briefing. This was published on our website on the day it was presented to the Minister. It is currently under consideration by the Government. We publish it in this report as **appendix 1**.

In essence our view is that proposals to share personal information between government agencies should be drawn up as agreed programmes, go through a process of consultation which will include consultation with the Privacy Commissioner, and be submitted for final approval by Order in Council. A new part of the Privacy Act would lay down the process. It would contain a statement of matters which would need to be covered in the programme and the criteria for approval. It would also prescribe transparency requirements: approved programmes would need to be published, a list of them should be contained in a schedule to the Privacy Act, and there should be reports on their operation. Appendix 1 also discusses some important questions, such as whether non-governmental organisations should come within the scope of this sharing regime, and whether *all* sharing programmes between government agencies should require approval, or only those which involve variation of the Privacy Act's principles.

Another question is what will happen to information matching if our proposals about information sharing are accepted. In our view, information matching is just a subset of information sharing, and it is a subset which is very hard to define with precision. Since the inception of the Privacy Act, information matching has been dealt with by a special statutory regime in the Act. Matching programmes are authorised individually by special statutory provisions, and once in place are subject to strict reporting and monitoring requirements. It is our view that if government accepts our information sharing proposals, information matching should simply merge into that new framework, and be subject to

the new rules. But, in case our proposals on information sharing are not accepted and the matching rules stay in the Act, we set out in **appendix 2** our recommendations for some (relatively technical) amendments to those rules.

Appendix 3 sets out in full the information privacy principles from section 6 of the Privacy Act. It also sets out sections 27 to 29 of the Act. These sections list the grounds on which access to personal information may be refused and are, in effect, exceptions to privacy principle 6.

Appendix 4 is a list of those who made submissions on the issues paper.

Appendix 1
Information sharing

This is the Ministerial Briefing issued by the Law Commission on 29 March 2011.

1 The Law Commission is currently engaged in a review of the Law of Privacy. The work is proceeding in four stages. The first three stages are complete,[819] and the Commission will soon complete the fourth and final stage, a review of the Privacy Act 1993. It published an Issues Paper on the subject in 2010, and is presently writing its final report. That report is due for publication by mid-year 2011.

2 In the course of the review of the Privacy Act we were asked to study the sharing of personal information between government agencies. The question is the extent to which a government agency that holds personal information about an individual is justified in disclosing that information to another agency. There has been uncertainty and debate about this subject for a number of years. Sharing is lawful now if it comes within one of the exceptions to the Privacy Act principles. Unfortunately, however, it is not always easy to get agreement between agencies on what is permissible and what is not. The whole-of-government solutions which can be facilitated by information sharing have attractions in many contexts, but they do have implications for the privacy of the individual, and it is no easy task to get the balance right.

3 In its Issues Paper on the review of the Privacy Act the Commission reviewed the literature and overseas developments, and put forward a number of options for taking the matter forward in this country. That work is contained in Chapter 10 of the Issues Paper. We received some helpful submissions on the options presented there. We have also consulted government agencies and others, and organised and participated in a number of forums where we put forward for comment the conclusions we have arrived at. We have also met, and exchanged ideas, with a group convened by the State Services Commission which has been working on the same topic.

819 Stage one of the review of the Law of Privacy was a high-level analysis to assess privacy values, changes in technology, international trends, and their implications for New Zealand law. Stage two was a consideration of the law relating to Public Registers and whether it requires systematic alteration as a result of privacy considerations and emerging technology. Stage three considered the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy.

4 Our conclusions and recommendations will be contained in a chapter of our final report on the review of the Privacy Act. However there is some urgency in the matter of information sharing, and we have been requested by the Minister Responsible for the Law Commission to present our conclusions, and eventual recommendations, in advance of that final report. This paper, which takes the form of policy advice to the Minister, fulfils that purpose.

5 In this paper we set out the reasons we believe reform of the law is required, and the principles on which that reform should be based. After discussing other options, we introduce our preferred option and discuss it in some detail. This is the "approved sharing programme". Sharing arrangements between agencies would go through an approval process culminating in approval by Order in Council, and would be listed in a schedule to the Privacy Act. The approval process would ensure that there was clarity as to what information could be disclosed, and that proper safeguards were in place to protect the privacy of the individual.

DEFINITION

6 We define the term "sharing" broadly as the disclosure of personal information about an individual by one agency to another. It can take many forms, including:

- A reciprocal exchange of information between agencies.
- One or more agencies providing information to another agency.
- Several agencies pooling information (as in a common database) and making it available to each other.

7 The physical ability of agencies to share information about citizens has been greatly enhanced in recent times. This is an area where technological advances are hugely significant. The difficulties of locating and sharing personal information between public sector agencies that exist 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. Government agencies want to use this technology to deliver better services more efficiently. Collaboration between agencies using shared information can often provide such better, "smarter" services.

8 A number of sharing programmes operate now. An example is the Linwood Service Centre in Christchurch where a number of agencies, including Work and Income, Career Services, Housing New Zealand, the Ministry of Health and the Ministry of Education work together to provide services for individuals and/or families with multiple service needs. Another is the Priority Offenders Initiative where Police, Probation and Prison Re-integration Officers, Housing New Zealand, Ministry of Education, Child, Youth and Family, Ministry of Health and Work and Income provide services in relation to frequent offenders who commit a disproportionate amount of crime in their local area. Another example, different again, is the projected Joint Border Management System

(JBMS) which is designed for the collection, storage and use of border information by the New Zealand Customs Service and the Ministry of Agriculture and Forestry.[820]

9 It will be immediately clear that the purposes of such arrangements, and the risks involved in them, differ considerably from one to another. Some focus exclusively on benefit to individuals and families; others are designed to benefit the community as a whole by preventing or detecting wrongdoing; others involve a mixture of both. Even in programmes that are ostensibly for the benefit of individuals things adverse to an individual may come to light to which the authorities cannot realistically be expected to turn a blind eye. There are difficulties, even dangers, in trying to classify sharing arrangements into pre-ordained categories.

10 As we shall explain in more detail later,[821] we think information matching, long regarded as a special type of activity subject to its own closely regulated regime, is really a form of sharing. We regard information sharing as a spectrum of different types of activity of which matching is one.

11 We note also that in this paper we are concerned only with sharing of information between agencies, and not with sharing between individuals in the same agency. That is a different question, albeit one which can raise its own issues, particularly where one agency has merged with another. We regard Privacy Act principles 5 and 10 as providing appropriate protection in that situation, but it may be that the transparency requirements that we propose later in this paper could have useful analogical application there too. We shall discuss intra-agency disclosures further in our report on the Review of the Privacy Act. Nor does our brief extend to sharing between New Zealand government agencies and overseas government agencies. We are concerned solely with sharing within New Zealand.

BENEFITS AND RISKS

12 Information sharing has obvious benefits. For individuals and families some types of sharing can, as in the case of the Linwood Centre, enable integrated assistance. Individuals are relieved of the need to supply the same information to several agencies. The agencies can work together to see and understand the individual's problems in their whole context, instead of each agency seeing only through its own narrowly focused lens. The Government, and therefore society, also benefit from the improved effectiveness of outcomes and from the efficiencies gained. Such activities should be facilitated. Other beneficial outcomes might include the more effective discovery and resolution of debts, and greater speed and certainty in ascertaining benefit entitlements. Sometimes the benefit of a co-ordinated response is so obvious that it goes without saying: the prevention of child abuse is a clear example; dealing with the aftermath of the devastating Christchurch earthquake is another.[822]

820 As provided for in the Customs and Excise (Joint Border Management Information Sharing and Other Matters) Amendment Bill 2010 which is awaiting its final stages in the House. Other examples of sharing initiatives are given in Issues Paper at [10.18]–[10.32], and in AMB Lips, RR O'Neill and EA Eppel *Improving Information Sharing for Effective Social Outcomes* (Victoria University of Wellington, December 2009) at 18 – 57.

821 See paragraphs [57]–[61].

822 The Privacy Commissioner has issued a temporary code of practice to facilitate sharing in that context: the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary).

13 However the risks of sharing can be considerable and need to be carefully managed. There are significant implications for individual privacy. Sharing, in fact, runs counter to two fundamental principles of the Privacy Act: that personal information should only be collected from the individual concerned, and that information collected for one purpose should not be used for another. Moreover, if information is inaccurate the error will appear in multiple databases, making it more difficult to correct. It may be difficult for individuals to find out exactly where their information is held so that they can take steps to ensure that it is corrected. Moreover some of the information shared can be particularly sensitive, information about finance and personal relationships for instance, and the more hands it passes through the greater the risk of its loss or misuse. Failures of security, the use of inaccurate information, and the use of information in ways which are not anticipated by the individual, can lead to loss of trust in government. The human psyche is instinctively fearful of the "big brother" state. No government can afford to lose the trust of its citizens: it will lead to reluctance to cooperate in providing information in the future.[823]

14 Privacy protection also has international significance. Government practices can have implications for cross-border dealings. As the UK Information Commissioner's Office has recently said: "Not only is personal information shared more often and in greater volume than ever before, but the potential for inadequate information handling systems and practices to have far reaching consequences has also increased dramatically."[824]

15 The authors of the Data Sharing Review Report in the UK sum it up this way:[825]

> 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.

THE NEED FOR REFORM

16 The question, therefore, is how to facilitate information sharing but also to ensure that proper protections and safeguards are in place. Much sharing is possible under the Privacy Act's information privacy principles (IPPs) now. Disclosure of information is often able to be justified as being within one of the exceptions to principle 11 (the non-disclosure principle), examples being the health and safety exception, and the maintenance of law exception.[826] Sharing is also justified if it is within the purpose for which the information was collected, or if the individual concerned has consented. We have heard a view that the Act is adequate as it stands and that with proper guidance the current IPPs are all that is required. We do not agree. It is quite difficult to fit some of the current sharing arrangements into the IPPs; the agencies involved often feel it necessary to get the consent of the individuals concerned rather than rely on the other exceptions. Moreover, the IPPs, and the exceptions to them, are expressed in

823 In AMB Lips, EA Eppel, A Cunningham and V Hopkins-Burns *Public Attitudes to the Sharing of Personal Information in the Course of Online Public Service Provisions* (Victoria University of Wellington, August 2010), the authors report on the results of research into public attitudes. They show that reaction depends on context, the extent of the sharing, and the population group in question.

824 Information Commissioner's Office *Response to the Ministry of Justice's call for evidence on the current data protection legislative framework* (6 October 2010) at 2.

825 R Thomas & M Walport *Data Sharing Review Report* (London, 2008) at 44.

826 Privacy Act 1993, s 6, Information Privacy Principle 11.

broad and open-ended terms, as they must be. But this means that they are open to differing interpretations. That is, perhaps, particularly so in the case of the purpose exception,[827] but all of them can from time to time give rise to uncertainty in their application.

17 Two things have resulted from this. First, agencies participating in sharing arrangements sometimes disagree on what is permissible and what is not. In our Issues Paper we summarised some of the conclusions reached by researchers from the Victoria University of Wellington:[828]

- Where agencies had a public safety mandate the Privacy Act was not seen as such an obstacle, with Principle 11 seen as providing adequate authority to share information. But 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 general 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.

We have heard in the strongest terms from agencies that things are unlikely to improve until there are clear detailed provisions to which agencies can point as justifying their actions.[829] Then there can be no argument as to what can and cannot be accessed. In this regard, Schedule 5 of the Privacy Act is seen as a useful precedent: it lists various types of information relating to law enforcement, and specifies the agencies which may access each type.

18 Secondly, rather than relying on the Privacy Act's existing provisions, some agencies are seeking specific amendments to their own Acts to validate particular sharing programmes. In our Issues Paper, we gave the examples of sections 181A and 182A of the Corrections Act 2004, which provide for information sharing about high-risk offenders and child sex offenders, and section 283 of the Accident 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 where that is necessary to protect children and young persons. In 2010 there have been two further examples: a Bill to enable Inland Revenue to share taxation information with other departments,[830] and a Bill to amend the Customs and Excise Act to enable the Customs Service and the Ministry of Agriculture and Forestry to share

827 Privacy Act 1993, s 6, Information Privacy Principle 11, and the first exception to it, read:

> 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.

The concept of the purpose of obtaining (as opposed to collecting) information may not always be crystal clear; "direct relation" to such a purpose can be a matter on which judgments may differ.

828 See Issues Paper at [10.58]. The Research Report is Lips, O'Neill and Eppel, above n 820.

829 From personal interviews, forums and seminar discussion.

830 Taxation (Tax Administration and Remedial Matters) Bill 2010 (257–1).

border information.[831] This process of specific statutory amendment is resource-intensive and time-consuming. In addition, there is currently no authoritative framework for assessing such proposals. The more this happens the more there is a risk of inconsistency and a loss of clear principle.

19 As we indicated above, some of the current sharing programmes operate with the consent of the individual. While this is certainly in accordance with the IPPs, it is not always satisfactory. It is one thing for a person to sign a detailed consent form, but another for that person to fully understand what it is that he or she is supposedly consenting to. We have also had it put to us that imbalance of power can be a significant problem in such cases. Moreover, a programme cannot operate with optimal effect if some individuals refuse their consent.

20 So we are of the view that reform is required to attain greater certainty in this area, and to ensure that proper safeguards are in place. Our aim is to identify a way to facilitate appropriate public sector information sharing within a framework of openness, transparency and accountability, which accords appropriate weight to privacy values.

OVERSEAS DEVELOPMENTS

21 In the Law Commission's Issues Paper we describe developments in information sharing in other jurisdictions similar to our own, with a warning that it can be dangerous to rely too heavily on overseas experience. Laws, and the culture surrounding them, can differ from place to place.

22 We now briefly summarise those developments. A fuller account can be found in the Issues Paper.[832]

23 All jurisdictions allow a disclosure of information which is within the purpose for which it was collected, or which has the consent of the individual. Beyond that, there is a great variety of provisions. In the **United Kingdom**, the lack of clarity in the relevant legislation has been a constant theme. A report published in 2008 recommended a statutory duty in the Information Commissioner to publish and update a code of practice relating to information sharing.[833] It also recommended a fast-track legislative procedure which would enable the Secretary of State, in precisely defined circumstances, to make orders removing or modifying barriers to information sharing. Such an order could amend primary legislation where necessary. Both Houses of Parliament would need to confirm the order by affirmative resolution before it became law. A Bill was introduced to implement these recommendations. The code-making power was passed into law, but the power in the Secretary of State to make orders was withdrawn from the Bill as a result of public outcry condemning the new powers as a dangerous threat to privacy.[834] The Information Commissioner released a draft code on information sharing for consultation in October 2010.

831 Customs and Excise (Joint Border Management Information Sharing and Other Matters) Amendment Bill 2010 (200–2).

832 Issues Paper at [10.68]–[10.115].

833 Thomas & Walport, above n 825, at 3.

834 The UK position is more fully discussed in Issues Paper at [10.71]–[10.87].

24 In **Canada** the federal legislation contains no specific provision relating to information sharing, although there is a broad power in a government institution to disclose personal information for a purpose where the public interest in disclosure clearly outweighs any invasion of privacy, or disclosure would clearly benefit the individual concerned. In New Brunswick the legislation provides that a public body may disclose information for any one of 24 specific, narrow purposes.[835] Both Alberta and British Columbia permit disclosure in a range of narrowly defined circumstances, but also where the information is necessary for the performance of the duties of an officer or employee of a public body, or where disclosure is necessary for the delivery of a "common or integrated" programme or service.[836] We return later to this concept, which we think holds promise.

25 In **Australia**,[837] the government has adopted a non-legislative National Government Information Sharing Strategy (NGISS). It emphasises the importance of a culture of collaboration, but also the need to take privacy into account. The Privacy Act 1988 (Cth) also empowers the Privacy Commissioner to make public interest determinations (PIDs), which might allow sharing in particular circumstances: these lie somewhere between codes of practice and section 54 exemptions under the New Zealand Privacy Act. The Commissioner must be satisfied that the public interest in engaging in the practice outweighs to a substantial degree the public interest in adhering to the privacy principles.

26 In New South Wales the Privacy Commissioner may, with the approval of the relevant minister, make a direction exempting an agency from complying with a privacy principle: this power has been used to enable agencies to exchange personal information. Similar exempting powers are available in the Northern Territory, Queensland and Tasmania: in each case an exemption can only be granted if the public interest outweighs the individual interest in privacy.

27 In **Ireland** in 2008 a report on transforming public services noted the need for legislative change to facilitate information sharing. To date there appears to have been no action.[838]

THE PRINCIPLES FOR REFORM

28 In our Issues Paper[839] we suggested five principles to guide reform. They are based on similar principles contained in a 2008 UK report.[840] There was general agreement with them on the part of submitters to our Issues Paper. In summary they are:

(a) Information sharing initiatives should be judged on a case-by-case basis. It is not a case of "one size fits all". Each sharing programme is different.

(b) There should be proportionality. The extent of the sharing should be neither greater nor lesser than necessary to meet the purpose. One should not use a sledgehammer to crack a nut.

835 Right to Information and Protection of Privacy Act RSNB 2009 c R-10.6, s 46.

836 Right to Information and Protection of Privacy Act RSA 2000 c F-25, s 40(1); Freedom of Information and Protection of Privacy Act RSBC 1996 c 165, s 33.2.

837 More detailed discussion of the position in Australia is contained in Issues Paper at [10.97]–[10.113].

838 Issues Paper at [10.114]–[10.115].

839 Ibid, at [10.116]–[10.123].

840 Thomas & Walport, above n 825.

(c) The risks of sharing must be managed, in particular the risks to individual privacy.

(d) Agencies must be held accountable if something goes wrong.

(e) There must be transparency, so that people know what is happening to their information. It is destructive of trust if information gets into other hands or is used for purposes that the individual did not know about.

SOME OPTIONS CONSIDERED

29 In our Issues Paper we put forward a number of options for reform. The reaction to them, and discussion of them, by submitters on the Issues Paper have enabled us to dismiss a number of the options from further consideration. We briefly summarise the most significant of those options and our conclusions about them after considering the submissions and the views expressed in subsequent consultations.

Options not requiring amendment to the Privacy Act

30 **First**, a set of guidelines, whether prepared by the Office of the Privacy Commissioner (OPC), or by another agency in consultation with OPC, as to what is now possible under the Privacy Act principles would be very helpful.[841] However we think that guidelines on the present operation of the principles are not enough alone. As we have said, every sharing programme is different. Guidelines must of necessity be at a fairly high level of generality and may not resolve some of the uncertainties about particular arrangements. Nor can guidelines vary the information privacy principles. So we believe that something more than guidelines is necessary. We do not wish, however, to be taken as undervaluing guidelines. If our recommended option is accepted, we would expect that guidelines would be prepared to assist in its operation. They might be prepared by OPC, but it might be just as valuable for them to be prepared by a cross-agency group.

31 **Secondly**, another possibility put forward in the Issues Paper was the formulation and publication of a government national strategy on information sharing.[842] This is subject to much the same reservation as the guidelines solution. Such a strategy would operate at a high level of generality, and it is hard to see how it could give the specific guidance needed for individual programmes. Nor could a non-legislated strategy change the law.

32 **Thirdly**, a Code of Practice relating to sharing made by the Privacy Commissioner under her statutory powers[843] remains a possible option, but a general sharing code would (again) have to be at a high level of generality, so it would probably be necessary to formulate a number of specific codes for particular sharing activities. The principle that sharing should be assessed on a case-by-case basis militates against the formulation of codes for "categories" of sharing. Even a code for the "welfare" sector might be too wide (what exactly constitutes "welfare"?).[844] The preparation of codes is resource intensive. OPC has to date not favoured this solution. So we do not put codes forward as a best option, although they remain a possible one.

841 Issues Paper at [10.128]–[10.132].

842 Ibid, at [10.136]–[10.140].

843 Ibid, at [10.133]–[10.135].

844 See para [35] below.

33 **Fourthly**, the Privacy Commissioner has power under section 54 of the Privacy Act to grant exemptions, or waivers, from the principles.[845] It would in theory be possible to "authorise" particular sharing programmes in this way. However there was very little support for this option. Section 54 is focussed on "one-off" exemptions rather than continuing programmes. Moreover, its use in this new context would effectively amount to a substitution of new rules rather than an exemption, and would not be very different from the code-making power.

Options requiring amendment to the Privacy Act

34 **First**, it may be possible to improve the current situation by making minor amendments to some of the exceptions to the principles. One that commands considerable support is to remove the word "imminent" from the exception to principles 10 and 11 which allows use or disclosure when that is:[846]

> 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.

A threat can be serious, and thus require preventing or lessening, even though it is not likely to eventuate on the instant. The Commission is likely to recommend such an amendment in its Report on the Review of the Privacy Act. The amendment would delete the word "imminent", and provide that in determining whether a threat is "serious", regard should be had to such matters as the likelihood that it will eventuate, the nature of the consequences if it does eventuate, and the time at which it may eventuate. In that way, imminence would not be a necessary condition, but simply one matter to be taken into account. Obviously, however, such a specific amendment would solve only a small part of the problem.

35 **Secondly**, we also floated in the Issues Paper the idea of including a "welfare" exception.[847] It might be added to the existing health and safety exception to cover a threat to "health, safety or welfare". There is precedent in Victorian legislation, and in a Bill in Western Australia.[848] While there was a little support for this in submissions, there was opposition too. We do not favour this option. "Welfare" is altogether too vague. It can mean different things to different people. Moreover, what is to one person's welfare may be to another's disadvantage. If one extended it to include the welfare of society as a whole in addition to the welfare of an individual, as some would like, all shape would be lost. Such an exception would open the door far too wide. It would be extremely difficult to police it.

845 Issues Paper at [4.92]–[4.97].

846 Ibid, at [10.190]; Privacy Act 1993, s 6.

847 Issues Paper at [10.190]–[10.191].

848 Discussed in ibid, at [10.190]–[10.191] and also at [10.113].

36 **Thirdly**, another option put forward in the Issues Paper was a "public sector as a single agency" provision.[849] It was presented in the form of a general presumption that information supplied to one agency 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. This received a mixed reception in submissions. We think it is too ill-defined, and consequently do not support it. What is a "broadly similar" purpose? When can it be said that a purpose is "beneficial to the individual"? We felt such a provision could generate fear that personal information provided to one agency would automatically be available across the board to other agencies: public confidence would not be enhanced by such a provision. We have emphasised the importance of trust: this kind of provision could do considerable damage to trust.

37 **Fourthly**, we also presented an option of amending the Act to allow the Privacy Commissioner to make binding rulings that programmes meet, or do not meet, the requirements of the Privacy Act.[850] This option attracted very little support. There were concerns about its relationship with the complaints process. Moreover privacy cases are very fact-specific and it may not be appropriate for rulings on one set of facts to be binding on others. Furthermore, such a solution could do no more than validate activities that were already Privacy Act compliant. We are not pursuing this option.

THREE PRELIMINARY POINTS

38 Before proceeding to discuss our preferred option, we would re-emphasise three points. First, whatever solution is adopted there will always remain room for guidance, from OPC as well as other agencies. There is already much valuable guidance on OPC's website: it is one of OPC's statutory functions to provide it. Guidance is not law and does not have binding force. No doubt whatever solution is finally provided for the problem of sharing, OPC guidelines can enhance it, and the understanding of it, just as it can clarify what is allowed under the existing principles and the exceptions to them. Secondly, in our report on the Privacy Act we shall be examining in detail the question of whether some of the existing principles and the exceptions to them need refinement. We noted in paragraph 34 the amendment to the "health and safety" exception that we are likely to recommend. Such amendments of detail could take place in addition to our preferred option. Thirdly, law reform alone will not solve all the problems which are currently apparent. Changes in culture and organisation will also be required. But we believe law reform is a necessary condition.

849 Ibid, at [10.141]–[10.148].

850 Ibid, at [10.149]–[10.174].

PREFERRED OPTION: THE APPROVED SHARING PROGRAMME

39 We now discuss the option that we prefer. It is in fact an amalgam of two of the options set out in the Issues Paper, both of which received substantial support from submitters.[851] We have also presented the idea at a number of forums and round-table discussions with agencies. It received significant support in principle on those occasions.

40 We believe that the greatest promise is held by the concept of an "approved sharing programme". In two Canadian provinces, Alberta and British Columbia, one of the statutory exceptions to the non-disclosure principle is "a common or integrated programme or service".[852] In neither Act is this phrase defined; instead its meaning is spelt out in guidance. The detail is, as it were, below the surface. Examples given in the Alberta guidelines suggest that the concept is principally focussed on programmes of beneficial service of the Linwood Service Centre kind.[853]

41 We think that for New Zealand the Canadian concept should be extended in two ways. First, we think that the exception should cover all types of sharing programmes and not just "beneficial service" programmes. In fact we think it would be quite difficult to isolate such a category. The solution we propose would be a general one which would cover programmes whose sole purpose is to provide holistic service to an individual or family; programmes which envisage the taking of adverse action against an individual; programmes which combine both these things; and programmes which raise at least the possibility that both may be involved. It would also include programmes which are presently dealt with as information matching. In other words, the concept should be the broad one of an "approved information sharing programme". Secondly, we believe that such programmes should require formal approval by Order in Council, and that legislation should lay down explicit rules for that approval, and clearly prescribe the protections which surround such programmes. Only in this way can the risks that attach to sharing programmes be sufficiently managed and solutions to them be prescribed. The types of programme are likely to vary considerably. Some would involve more agencies, more information, and more risks than others. Some might modify the application of one or more of the information privacy principles in the Privacy Act. The safeguards and checks and balances would need to be proportionate to those varying levels of risk.

42 In essence what we are proposing is a system whereby agencies proposing a sharing arrangement would draw up an agreement (or protocol); that agreement would be subject to an approval process culminating in approval by Order in Council; and the approved programme would be publicly notified and included in a schedule to the Privacy Act. By that process agencies can have certainty, and can demonstrate to the public that what they are doing is permitted by law even though there might otherwise have been an argument that the principles in the Privacy Act did not cover the activity. There will also be an assurance that threats to privacy have been identified and appropriately managed.

851 Ibid, at [10.198]–[10.203] and [10.208]–[10.221].

852 Ibid, at [10.89]–[10.96], discussing Right to Information and Protection of Privacy Act RSA 2000 c F-25 and Freedom of Information and Protection of Privacy Act RSBC 1996 c 165.

853 Access and Privacy Service Alberta "Common or Integrated Programmes or Services" (March 2009) *foip bulletin* 8

43 We believe that the new machinery should be contained in a separate part of the Privacy Act dealing with the sharing of personal information between government agencies. We do not favour the solution of a separate "Information Sharing" Act. That way the privacy implications could too easily be forgotten. The Privacy Commissioner will have an important role to play, and the new provisions should be in the same Act that lays down the Commissioner's functions. Moreover, the provisions about information matching, which we see as a special form of sharing, are currently located in the Privacy Act.

44 The legislative provisions would deal with the following matters. In formulating these criteria we have worked from first principles, but have also been guided by the current rules about information matching (suitably adapted to the less formal context) and the proposed provisions of a Bill currently before Parliament.[854]

Approval

45 There should be a statutorily prescribed process for establishing sharing programmes. The two or more agencies involved would prepare a written agreement containing the details of the proposed sharing programme. In preparing it they would be required to consult with appropriate persons and agencies: OPC would be able to recommend, and the relevant ministers to require, that certain persons be included in the consultation. Some programmes would obviously require more consultation than others. Consultation with OPC would be mandatory. In the case of more extensive programmes OPC might require that a privacy impact assessment be undertaken.

46 The programme would then be signed off by the relevant portfolio ministers and would be submitted to Cabinet for approval. A report from OPC would be considered by Cabinet as part of the approval process; that OPC report should be a public document.

47 The criteria for approval should be:

- That the purpose of the programme is to achieve a significant benefit to society or to individuals. "Benefit" may include, but is not confined to, economic benefit.
- That the benefit to be achieved by the programme outweighs the risks involved, in particular the risks to individual privacy.
- That the type and quantity of information to be shared, and the number of agencies involved, are necessary for the attainment of the purpose of the programme.
- That the safeguards contained in the programme agreement are adequate and proportionate to the risks involved.
- That the programme agreement provides for the matters prescribed by the Act.

854 See the Privacy Act 1993, Part 10 and sch 4; also the Customs and Excise (Joint Border Management Information Sharing and Other Matters) Amendment Bill 2010 (200–2), cl 25 adding new s 286A to the principal Act.

Before approving a programme Cabinet would be required to take into account:

- The degree to which the proposed programme departs from the information privacy principles in the Privacy Act.
- Whether there are other ways of achieving the desired purpose, and whether the proposed programme is the best way (the agencies involved would need, in other words, to explain the options they had considered).
- The results of the consultation process and any recommendations of OPC.

Contents of agreement

48 The Act should provide that the agreement between the agencies must contain the following:

- A clear statement of the purpose of the programme.
- A clear statement of the category or categories of personal information which may be shared. (These should be stated with some specificity. It will not be enough to provide for open-ended ill-defined categories of information.)
- A list by name of the agencies participating in the programme and the types of information to which each is entitled. Not all agencies might necessarily be entitled to all types of information. There should be provision that if agencies later change their names, or if their functions are transferred to other agencies, the list in the agreement will be read as referring to the up-to-date version.
- A clear statement of the uses to which a recipient agency may put the information.
- A requirement to establish and maintain detailed technical standards.
- A description of the safeguards to be adopted to ensure security of the information shared. The more sensitive the information the higher will be the required level of security.
- Details of how the general requirements of the Privacy Act relating to sharing programmes are to be met.
- The nomination of one agency as the lead agency (to prevent confusion about responsibility for such things as reporting).

49 It may be possible for model template sharing agreements to be prepared – perhaps by OPC or the State Services Commission – to serve as a guide. However any template would need to be modified for the purpose of an individual programme; we recall the principle that sharing activities must be assessed on a case-by-case basis. We would also expect guidance to be available as to the appropriate level of safeguards for various categories of agreement.

General rules applying to all programmes

50 The Act should also contain some mandatory general requirements which would apply to all sharing programmes.[855] It should provide as follows:

855 Again, some of these requirements have been adapted from the current matching provisions.

(a) Safeguards

(i) Information subject to a sharing programme may only be used by, or disclosed to, agencies participating in the programme and for the purposes stated in the programme. However, there would need to be an exception to this to deal with exceptional situations where either the health and safety or maintenance of the law exception required it. Information could then be disclosed to the agency appropriate to deal with it.

(ii) If as a result of an information sharing programme information is discovered that results in the need to take adverse action against an individual, the individual must be given a period of notice and an opportunity to object to the proposed action. Adverse action would be defined as in the current matching provisions of the Privacy Act[856], but with the addition of a decision to impose a penalty and a decision to recover a penalty or fine earlier imposed. The period of notice should be at least ten days, although with power in the Privacy Commissioner to approve a lesser period in particular circumstances. There would need also to be an exception to the requirement of notice if action is urgently required as it might be, for example, in a case of child abuse or domestic violence. The time limit for commencing adverse action should be 12 months, as it currently is for information matching.[857]

(iii) Information obtained by an agency in the course of an information sharing programme must not be kept for longer than necessary for the purposes of the programme.

(b) Transparency

The Privacy Act is itself based on the premise that individuals have a right to know what information is held about them, and the purposes for which it is being used. The proposed legislation should expand on the application of those principles to sharing arrangements. It should provide as follows:

(i) Agencies involved in a sharing programme must take all reasonable and practicable steps to ensure that the individuals subject to the programme are notified of it.

(ii) The text of an approved programme agreement must be published on the website of the lead agency, with links on the websites of the other participating agencies. Individuals who are, or could be, affected will then know which agencies may hold their information, and can if they wish exercise their right under principle 6 of the Privacy Act to have access to it.

(iii) The lead agency must report annually on the operation of the programme. In most cases it would be enough to have this report as one part of the agency's annual report, but in appropriate instances it might be made a condition of the initial approval of the programme that the report be made to OPC as well. If concerns later develop about the operation of a programme OPC should also be able to request a report to them.

856 Privacy Act 1993, s 97.

857 Privacy Act 1993, s 101(2).

(iv) On the approval of each programme it should be added by Order in Council to a schedule of the Privacy Act. In this way the number and nature of all existing programmes could be seen at a glance. Ideally the schedule would follow much the same form as the present Schedule 5 (the Law Enforcement schedule) and would indicate the agencies involved, the type of information shared, and the purpose of the sharing. Such a schedule would provide information for the public, and ready assurance for agencies and others that what the agencies are doing is permitted by law. In a sense this power to add to a schedule by Order in Council may look like what is sometimes called a Henry VIII clause.[858] But the purpose of such additions to the schedule would just be to provide information: they would record the result of a statutorily authorized process. In that sense the procedure is no more exceptional than several other provisions which allow statutory amendment by Order in Council.[859]

(c) Accountability

A breach of any of the provisions of the Act relating to sharing programmes and/or a breach of any of the terms of an approved programme would, provided the statutory harm threshold was reached, constitute an interference with privacy and thus be a ground of complaint to the Office of the Privacy Commissioner. The Act would need to make express provision to this effect. Currently the Commissioner attempts to resolve complaints by a process of mediation or negotiation. Those which cannot be resolved in this way may proceed to the Human Rights Review Tribunal. In our forthcoming report on the review of the Privacy Act we shall investigate whether the Privacy Commissioner should have greater powers to enforce compliance.

(d) Parliamentary oversight

Parliamentary enactment for each sharing programme is not envisaged, but it is desirable that the process be subject to parliamentary oversight. The Orders in Council approving programmes should be disallowable instruments under the Regulations (Disallowance) Act 1989. They would be subject to the scrutiny of the Regulations Review Committee. That committee would apply the grounds in Standing Orders for drawing a regulation to the attention of the House, among them that it trespasses unduly on personal rights and liberties, or that it makes unusual or unexpected use of the statutory powers.

(e) Review

For resource reasons we do not suggest that programmes be subject to mandatory review after any set period of years, but if any annual report, or other evidence, indicated that a particular programme was not working satisfactorily, or that it was no longer required, or that its purpose had changed, OPC could initiate a review of it. (Such a review might indicate that the programme should be formally amended.) On the other hand, we do think that the new statutory

858 See Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (May 2001) at [10.1.8].

859 See for example Misuse of Drugs Act 1975, s 4. Compare Education Act 1989, s 162(2), which enables the Governor-General by Order in Council to establish new universities without the need even to add them to the list of existing universities in schedule 13.

framework we are proposing should be reviewed after the first three years. Given the speed of developments in technology, and the importance of information sharing for both individuals and society, it is desirable that the operation of the new process be examined to ensure that it remains fit for purpose. There should be provision in the Act for such a review by a person or body nominated by the Minister. OPC should be centrally involved in such a review.

DISCUSSION

51 In our view this proposal satisfies the five principles we have outlined in paragraph 28 above. In some cases the sharing provided for in an approved programme might be permissible already under the principles in the Privacy Act and the exceptions to them. In such a case the approval of the programme would give the participating agencies a confidence and certainty they may not have had previously. On the other hand, in other cases the activities might, arguably, not be protected under the Privacy Act as it currently stands. In that case the approved programme would validate sharing that might otherwise have been open to question.

52 The essential feature of the proposal is the approval of each individual sharing programme by Order in Council. There may be some who believe that sharing programmes involve such significant risk that they should be specifically authorised only by Act of Parliament, as is effectively the case now with matching programmes. It might be argued that given the potential threat to individual rights specific authorisation by Parliament itself is more appropriate. However we think Order in Council is the preferable vehicle. Parliamentary time is a scarce resource, and the delays involved in getting the appropriate Bill on the Parliamentary agenda and in getting the Bill passed would be highly undesirable. Provided the Privacy Act itself contains carefully formulated rules of the kind we have outlined the safeguards should be adequate. They include the consultation process; the involvement of OPC and the publicity of the OPC report; the transparency requirements; and the possibility of disallowance. Given that Cabinet processes are not as open as Parliament's, it is clear that there need to be such safeguards.

53 Nor is the Order in Council route contrary to the general scheme of the Privacy Act. Although the Act does currently provide for the statutory creation of matching programmes and also the statutory addition of items to Schedule 5, it also confers very considerable power on the Privacy Commissioner to make delegated legislation in the form of codes, albeit subject to a prescribed consultation process. Those codes can vary the statutory privacy principles. To authorise the approval of sharing programmes by the Order in Council process is not, it seems to us, out of place in that statutory context.

54 However this is not to exclude the possibility that there may be situations where special far-reaching measures are necessary, and where special legislation may be the most appropriate vehicle. An example might be a situation where it is felt necessary to impose enforceable *duties* to disclose information to protect a particular category of vulnerable person.

55 On the other hand, there may be some who view the Order in Council process as overly bureaucratic. Some might prefer a more streamlined procedure. We agree that there should not be unnecessary bureaucracy, and that the imposition of burdensome procedural hurdles would deter agencies. But we do not think that what we propose creates unreasonable burdens. One would hope that any sharing arrangement would even now be accompanied by a careful written protocol, and that the Privacy Commissioner would be consulted. One would also hope that risks were properly managed. A Chief Executive should properly insist on that. The suggested procedure only ensures that this will happen, and involves the further step of Cabinet approval to ensure independent scrutiny. The requirement of transparency is also no more than good practice should already require. Transparency is a basic tenet of the information privacy principles.

TWO CURRENT ARRANGEMENTS

56 At present the Privacy Act makes provision for two activities which are effectively types of information sharing: these are information matching and access to law enforcement information. The question is how these two existing sorts of arrangement will fit with the proposed regime for information sharing.

Information matching

57 We have carefully considered the matter of information matching. That is currently the subject of a statutory regime which has been in the Privacy Act from the beginning.[860] Matching programmes are individually authorised by specific provisions in Acts of Parliament. OPC has the function of assessing proposals for such statutory authorities against a set of guidelines contained in the Privacy Act.[861] Once a matching programme has been approved by its own separate Act of Parliament, a reference to that Act is added to a schedule to the Privacy Act (Schedule 3) and must be operated according to matching agreements approved by OPC; these agreements must comply with a set of rules contained in the Privacy Act.

58 It is our view that, provided adequate safeguards are included in the Privacy Act, it is best to treat information matching as a kind of sharing, and subject it to the same Order in Council regime as the other types of sharing. There is considerable uncertainty at the moment as to how matching is to be properly defined and as to how, if at all, it differs from sharing. The Privacy Act has two definitions of matching which at first sight bear little resemblance to each other.[862] They are the cause of considerable confusion. An **authorised information matching programme** means:

> the comparison (whether manually or by means of any electronic or other device) of authorised information matching information with other personal information for the purpose of producing or verifying information about an identifiable individual.

860 Indeed it predates the Privacy Act 1993, being first enacted in the Privacy Commissioner Act 1991, and then carried forward into the 1993 Act.

861 Privacy Act 1993, Part 10.

862 Privacy Act 1993, s 97.

On the other hand an **information matching programme** means:

> the comparison (whether manually or by means of any electronic or other device) of any document that contains personal information about 10 or more individuals with one or more other documents which contain personal information about 10 or more individuals for the purpose of producing or verifying information which may be used for the purpose of taking adverse action against an identifiable individual.

There is no internationally accepted definition of matching. A recent guide prepared by the Victorian Privacy Commissioner for the Victorian public sector says:[863]

> Although in common use the term "data matching" means different things to different people. No standard definition exists. Various activities involving the comparison of separate data sets may be referred to as data matching.

59 We have considered the possibility of ring-fencing a narrow type of matching within a precise definition and retaining the current Part 10 of the Privacy Act to deal with it. One might, for example, use the second and narrower "two sets of 10 persons" definition cited above. However, this would be artificially narrow and entirely arbitrary. There would be no point in it. The risks involved in this kind of "bulk matching" activity do not seem to be any greater than those involved in collating information about a known individual from a number of separate databases.

60 So we prefer to treat matching simply as one type of sharing, and to apply the same Order in Council process for programme approvals. The safeguards would, we believe, be just as effective as those currently applied. In fact a good number of the provisions we have recommended for sharing programmes are modelled on the Act's current matching regime.

61 There will be a question as to what happens to matching arrangements which were in force before the change. We believe they should simply be grandparented without any need to be re-approved, but in relation to their ongoing operation they should be subject to the new rules.

Schedule 5

62 Schedule 5 of the Privacy Act contains a list of agencies which can share law enforcement information, and the types of information which can be shared. In the early years the schedule could be added to by Order in Council, but now that is done by Act of Parliament.

63 The question is whether law enforcement is sufficiently distinct to have its own regime under schedule 5. We think not. While law enforcement information is sensitive, so are other types of information which we would envisage being included in sharing arrangements (for instance, child welfare and financial

863 Privacy Commissioner *Data Matching in the Public Interest: a Guide for the Victorian Public Sector* (August 2009) at 5.

information). Also, any exclusive regime for law enforcement could lead to confusion and difficulty in cases where a sharing arrangement involved both law enforcement information and other types of information.

64 We therefore propose that the new information sharing regime should encompass law enforcement information, and that there should no longer be a separate schedule 5. The arrangements in the present schedule 5 should be grandparented and transferred to the general information sharing schedule. New law enforcement arrangements should be subject to the new approval rules.

SCOPE

Types of programme

65 It would be totally unrealistic to require that all disclosure of personal information between government agencies must take place in accordance with a programme approved in the way, and by the process, that we have outlined. Sometimes it may be acceptable, even necessary, for one agency to supply information about an identified person to another so long as such supply is in accord with the Privacy Act's principles. If, for example, a dangerous psychiatric patient has escaped from confinement it would be absurd to suppose that the Ministry of Health could not immediately liaise with the Police. Ad hoc sharing of this kind, which is within the Privacy Act principles, must be allowable. Indeed, it does not involve a "programme" at all.

66 What we are concerned with in this paper is continuing *programmes* or *arrangements* for sharing which involve categories of information and groups of as yet unidentified individuals.

67 There are two options. **One** is that all such programmes should require formal approval. The basis for this would be that government agencies are in a unique relationship with their citizens where trust is particularly important, so that if they engage in the activity of sharing citizens' information they should get approval for it. All programmes would then be on the same basis, subject to the same checks and balances, and equally transparent.

68 The **second** option is that programme approval is only required if the programme is not compliant with the Privacy Act principles and their exceptions. This would, in a sense, give the agencies some discretion. They *might* decide to apply for approval even if the programme were Privacy Act-compliant; they would *have* to do so if it were not compliant; and would be strongly *advised* to do so if there was uncertainty or disagreement about whether it was compliant or not.

69 It should be noted that currently it appears to be possible to match information without going through the process set out in Part 10 of the Act: there is no provision in the Privacy Act explicitly saying that information matching requires statutory authorisation. Nor is schedule 5 the only avenue for accessing law enforcement information: it may sometimes be possible by simply relying on the "maintenance of the law" exception to the disclosure principle.

70 Of these options, we prefer the first. There would be some discomfort about having two sets of programmes, one approved and the other non-approved. It might engender unjustified suspicion of the non-approved. Moreover, agencies might wrongly assume that their programme was Privacy Act-compliant when in fact it was not, and thus fail to seek approval. The second option would also mean that the list of approved programmes in the schedule did not tell the whole story.

71 Yet, we acknowledge that the approval process will involve resources, and to require approval of all programmes would involve more resources than the second option. That would be so not just for agencies, but also for OPC, although it is not clear just how much greater the burden on OPC would be: it already spends a lot of time answering agency queries about the subject, and is heavily involved in all matching programmes. There is also something anomalous about requiring a formal process to be gone through in relation to activities which have been going on, perhaps for years, in full compliance with the Privacy Act.

72 So while we prefer the first option we would not oppose the second. But if the second is chosen, we believe that transparency should still be required. The agencies engaging in non-approved programmes should therefore be required to publicise them on their websites, and report on them annually. It would also be desirable for a list of such arrangements to be compiled and published on the internet by either the Ministry of Justice, or the State Services Commission, or the Office of the Privacy Commissioner.

Agencies

73 A further question is whether the new sharing programme rules should apply only to sharing between central government agencies or whether they should also include the private sector, non-governmental organisations (NGOs) and local government. This question is likely to be raised increasingly frequently in this new age where there is increasing talk about public-private partnerships. We note that the current matching rules in the Act apply only to "public sector agencies".

74 We are nervous about extending the approval processes that we are recommending to NGOs. For one thing, much work needs to be done in determining the preparedness and capacity of some NGOs to participate in sharing programmes, particularly in relation to their technical capacity. Moreover the question of trust is a particular issue in relation to NGOs. Many NGOs are charities that receive information from individuals in confidence. If an individual entrusts personal information to, say, the Salvation Army or the Plunket Society, he or she usually does not expect it to end up in the hands of a government department. We have discussed proposals for sharing programmes with a group of NGOs and, while their reactions differed, it was clear that some of them harboured considerable concern about this.

75 However, we understand that some "beneficial service" programmes do benefit from the involvement of NGOs and that in such cases the information the subject of the programme is usually supplied *to* the NGOs rather than being received *from* them. Provided a particular NGO can satisfy the security requirements – a matter for the programme approval process – we think it could become part of a sharing arrangement on the limited basis that we have indicated in this paragraph.

76 There may be cases, too, where it is proposed that an NGO should act solely as an *agent* for the government agency. In such a case it would be just as if the government agency was doing the job itself. This might also be acceptable, provided a provision in the Act made it clear that information in the hands of the NGO was deemed still to be held by the government agency, which remained responsible for the information, and accountable for anything that happened to it. It would be necessary to adapt the present section 3(4) of the Privacy Act to the purpose, or insert a new provision to similar effect.

77 With regard to the private sector and local authorities, however, we think that the proposed sharing programme process should be allowed time to bed in within the central government agencies before extending it thus far beyond them. It is often best to introduce new concepts and processes with caution, and not to open the door too wide from the outset.

78 Should the proposed system be adopted and come into being, it would still be possible to pass individual Acts of Parliament to authorise exceptional arrangements which go beyond what is currently proposed. Parliament is sovereign. There may be exceptional public-private partnerships which would justify such a solution. When the new system has been operating for a sufficient time for it to be possible to assess its operation, the general legislative framework here proposed could be amended to include additional classes of agency.

79 So our present view is that, with the limited exception for NGOs which we have outlined, the new sharing provisions should initially only apply to Ministers, departments and other organs of central government.

PROPOSALS

We thus propose:

(1) That the Privacy Act 1993 should be amended to make provision for the approval of programmes for the sharing of personal information between government agencies.

(2) That such programmes should require approval by Order in Council.

(3) That the Privacy Act should expressly lay down the process of approval, which would involve consultation with appropriate persons including the Privacy Commissioner; the criteria for approval; the matters required to be contained in programme agreements; and general rules for the operation of such programmes. The general rules should provide safeguards, require transparency, and provide for means of accountability.

(4) That Orders in Council approving programmes should be disallowable instruments within the Regulations (Disallowance) Act 1989.

(5) That information matching should be treated as a form of information sharing, and be subject to the same processes and rules. Existing matching programmes should not have to be re-approved, but in their ongoing operation they should be subject to the new rules. The same should be true of law enforcement information currently contained in schedule 5 of the Privacy Act.

(6) That the proposed regime should apply to all continuing programmes of information sharing between government agencies. If, however, it is decided that approval should be required only for programmes which are not otherwise compliant with the Privacy Act, the transparency requirements should apply to the non-approved programmes.

(7) That, in the first instance, the proposed regime should apply only to sharing between central government agencies, although in appropriate cases it might be extended to include non-governmental organisations on the basis described in paragraphs [75] and [76].

(8) That all approved programmes should be listed in a schedule to the Privacy Act 1993.

Appendix 2
Information matching

1 In appendix 1, we recommend that information matching should be seen as a type of information sharing, governed by the same rules. Insofar as some types of matching may carry greater risks, the safeguards to be included in the programme agreement would be proportionately greater.

2 However, if our proposals in appendix 1 are not accepted, we need to consider what should then happen with information matching, which would continue to be regulated separately. This appendix will consider that question.

3 First, if matching remains as a separate concept it will need to be defined. The two definitions which appear in section 97 – the definitions of "information matching programme"[864] and "authorised information matching programme"[865] – are poles apart, and have been the source of much confusion. There is debate and uncertainty, even among those who understand the information matching provisions, as to whether certain activities come under the umbrella of "information matching" at all. A single definition is necessary. In our view, much will depend on whether or not information sharing is to have its own regulatory regime separate from matching. If it is, we think "matching" should be defined narrowly, to cover only the relatively high-risk situations where it is thought that individual authorisation by Act of Parliament is desirable. We suggest that the present definition of "information matching programme" in section 97 would be appropriate: it deals with the "blind" matching of two groups of bulk data, where the resulting information may be used to take adverse action against individuals.

4 If, however, "sharing" is to have no regulated regime, then "matching" may need to cover more ground. In that case, the present definition of "authorised information matching programme" would be more appropriate. There would be more protection against privacy invasion.

---

864 **Information matching programme** means the comparison (whether manually or by means of any electronic or other device) of any document that contains personal information about 10 or more individuals with 1 or more other documents that contain personal information about 10 or more individuals, for the purpose of producing or verifying information that may be used for the purpose of taking adverse action against an identifiable individual.

865 **Authorised information matching programme** means the comparison (whether manually or by means of any electronic or other device) of authorised information matching information with other personal information for the purpose of producing or verifying information about an identifiable individual.

5 We asked in the issues paper whether the matching provisions should come out of the Privacy Act and be enacted in a stand-alone Act. There was little support for this in the submissions, and we do not support it. It is best for all the provisions about the handling of personal information to be together. Moreover, if matching were to be taken out of the context of the Privacy Act, its implications for privacy may not be sufficiently appreciated.

6 In our issues paper we asked a number of questions about the current matching regime. Those questions will remain relevant if our proposals in appendix 1 are not accepted. Even if those proposals are accepted, the decisions on a few of the questions will have implications for the new sharing regime.

7 We shall deal first with the issues on which we have decided to recommend no change.

RECOMMENDATIONS FOR NO CHANGE

8 First, we do not think there should be any amendment of the Privacy Act to the effect that the information matching regime should be extended to the private sector. If private sector entities are able to engage in limited matching activity consistently with the current privacy principles, they can do so without special authorisation. It would also be possible to make a code of practice regulating matching activities in the private sector.[866] Beyond that, we currently think there is no case for a statutory regime authorising the private sector to engage in activities which would otherwise be in contravention of the principles. Government agencies have a public function which is different in kind.

9 However, public-private partnership arrangements may sometimes raise different issues. We believe this is a question which should be visited when the Act is next reviewed. In the interim, should there need to be matching arrangements between public and private sector agencies to deal with matters of high public importance – the prevention of terrorism, for instance – they can be authorised by specific, specially tailored, Acts of Parliament.

10 Secondly, we asked in our issues paper whether the current controls on matching are appropriate. Most submitters thought they were. We have indeed adopted the key controls for wider use in our proposals for the sharing regime we recommend in appendix 1.

11 Thirdly, we asked whether the definition of "adverse action" in the notification provisions should be amended to clarify that programmes which have only beneficial consequences and no adverse ones are excluded. There was little support for such a move in submissions, and we do not support it. Such a provision would have no obvious purpose. Moreover, as we pointed out in appendix 1,[867] it would be difficult to find a matching programme which did not contain at least the *possibility* of adverse action.

866 Privacy Act 1993, s 46(4)(a).

867 Appendix 1 at [9].

12 Fourthly, we asked whether the information matching regime should be confined to computerised or automated matching.[868] There will these days be very few, if any, programmes which involve manual matching. But they could in theory still happen, and damage could be done if they are not properly regulated. No harm is done by leaving the provisions as they are. So the legislation should continue to apply to all sorts of matching, including manual.

13 Fifthly, we wondered whether there should be more transparency about "data mining" activities: whether, for example, there should be a reporting requirement.[869] Although some submissions supported this, we do not recommend it. "Data mining" covers a multitude of activities, and would be well-nigh impossible to define. Not only would a reporting requirement be a bureaucratic imposition, but some submissions made the point that it might also be harmful in that it would give publicity to techniques which others might wish to emulate or might take steps to counteract. We recommend that there be no change to the Act in this regard.

RECOMMENDATIONS FOR AMENDMENT

14 We believe that, if matching is to be retained as a separate category in the Act, there might be a few amendments to the rules which currently apply. Some of these proposed amendments are reflected in the controls we have recommended in appendix 1 for a new information sharing regime.

15 First, if it is proposed to take adverse action against someone as a result of information discovered in the course of a matching programme, currently five days' notice must be given to that person. In the issues paper we asked whether ten days might be more appropriate.[870] Five days is not very long: the notice may arrive when the person is away, or the person may need to take advice. Innocent people can be caught in the net by mistake, and need a proper opportunity to extricate themselves. Five days is short by comparison with some overseas jurisdictions. We think ten days is more appropriate. Notice might be given electronically or in hard copy.[871]

16 However, we acknowledge, as pointed out in several submissions, that such a lengthening of the period would not suit all situations. That is particularly so when a purpose of the programme is to stop the payment of benefits to which there is no entitlement. We therefore recommend that the period be ten days, but with power in the Privacy Commissioner to reduce the period in appropriate situations.

17 Secondly, there is a question of what, exactly, "adverse action" is.[872] The definition of the expression in section 97 gives seven examples, including cancelling or suspending a monetary payment, and deporting the individual or revoking his or her visa. There was general agreement in submissions that it would be helpful to add two more examples to the list: a decision to impose a penalty, and a decision to recover a penalty or fine. We so recommend.

868 Issues Paper at [9.122]–[9.124].

869 Ibid, at [9.58]–[9.70].

870 Ibid, at [9.132]–[9.135].

871 At present, Privacy Act 1993, s 103(3) is drafted in such a way that it does not seem to allow for the delivery of notice by electronic means.

872 Issues Paper at [9.115]–[9.124].

18 Thirdly, it would appear that it is possible at the moment to engage in information matching without having an authorised programme under Part 10. If it can be done within the privacy principles there appears to be no impediment.[873] There is, however, a limited exception. Section 108 provides as follows:

> **Avoidance of controls on information matching through use of exceptions to information privacy principles**
>
> Where the collection or disclosure of information is authorised by an information matching provision, nothing in subclause (2)(d)(i) of principle 2 or paragraph (e)(i) of principle 11 authorises or permits the collection or disclosure of that information for the purposes of
>
> (a) any authorised information matching programme; or
>
> (b) any information matching programme the objective of which is similar in nature to any authorised information matching programme.

19 It is not just that the position is complex and ill-understood. We believe that all *significant* information-matching activity by government agencies should be subject to the same rules, and more importantly that it should be *transparent*. Any ability to match information outside Part 10 of the Act enables it to be done "under the radar", as it were.

20 The majority of submitters also took that view. We therefore believe that while isolated one-off information disclosures within the concept of "matching" may be allowable provided they are within the privacy principles, any *continuing programme* of matching between government agencies should have to be authorised, and operate, under Part 10. That should be made express in the legislation.[874] It probably reflects the current general understanding. As we discuss in appendix 1,[875] this is our preferred solution for information sharing too, although we note in our discussion of that subject that if our recommendation is not accepted, there should nonetheless be transparency requirements for all programmes.

21 Fourthly, in the issues paper we asked whether there should be a statutory requirement for agencies seeking legislation authorising an information matching programme to provide the Privacy Commissioner with a protocol, to assist the Commissioner in commenting on the proposal.[876]

22 In essence, we were asking whether there should be a description of the detail of the proposed programme and the way it would operate in practice. It seems obvious that to make an informed assessment of a programme the Privacy Commissioner needs such a descriptive document, and most submitters agreed that it should be required. We think that in many cases the protocol could usefully be accompanied by a privacy impact assessment (PIA), and that the Privacy Commissioner should be able to require that where appropriate.

---

873 Ibid, at [9.32]–[9.35] and [9.111]–[9.114].

874 There would probably need to be an exemption for the intelligence organisations: compare Privacy Act 1993, s 57.

875 Appendix 1 at [65]–[72].

876 Issues Paper at [9.128]–[9.131].

23 In appendix 1 on information sharing, we similarly propose that, as part of the mandatory consultation with the Privacy Commissioner in the course of programme approval, he or she should be able to require a PIA.[877]

24 Fifthly, the Privacy Act currently requires a five-yearly review by OPC of every information matching provision.[878] It is apparent that the Commissioner has insufficient resources to meet that demanding timetable. We think the requirement of mandatory periodic review should be removed. Rather, the Commissioner should be able to conduct reviews if and when they are desirable. If an annual report were to reveal a problem with a particular programme, a review would be appropriate. With a permissive rather than mandatory review provision the Commissioner would be able, if he or she desired, to prepare a prioritised programme. We recommend similarly in appendix 1 on information sharing.[879] We are not generally in favour of sunset clauses in matching authorisations: they create as much work as reviews, and they are even more dependent on time deadlines. But were there to be a matching programme which involved particular sensitivity or risk, it would be open to Parliament to include a sunset clause in the specific legislative provision which authorised it.

25 Sixthly, whether or not our previous recommendation is adopted, the Privacy Commissioner may, from time to time, conduct reviews of information matching authorities and may recommend amendments to them. We believe, and most submitters to the issues paper agree, that there should be a requirement that the government respond to the report within six months of its presentation.

26 Seventhly, the Privacy Commissioner must currently include in his or her annual report a report on his or her monitoring of matching programmes. In *Necessary and Desirable*,[880] the Privacy Commissioner recommended delinking the annual report from the information matching report, since finalisation of OPC's annual report can be unnecessarily delayed while waiting for the information matching reports to be received from agencies and analysed by OPC. It was proposed that the Commissioner's report on the information matching programmes would be presented separately to Parliament.[881] We agree, and so recommend.

27 Eighthly, the information matching rules are at present in schedule 4 of the Privacy Act. Information matching agreements between agencies must contain provisions which reflect those rules. The rules contain provisions of considerable substantive importance, some particularly so: for instance, the requirements that reasonable steps be taken to notify individuals, and that unique identifiers not be used unless their use is essential. We believe that the rules would be better placed in the body of the Act. However, we think that rule 3, which relates to online transfers, has outlived its usefulness. Such a provision was understandable in 1991 when such transfers were out of the ordinary, but has

877 Appendix 1 at [45].

878 Issues Paper at [9.138]–[9.141].

879 Appendix 1 at [50(e)].

880 *Necessary and Desirable*, recommendation 131.

881 Issues Paper at [9.137].

no justification in 2011. Security of transfer is the main issue, and that is covered in rule 4(2)(d). We thus believe that rule 3 should be deleted. We believe also that rule 8, requiring agencies to establish limits on the number of times that matching is carried out each year, is too rigid. There is bound to be an element of arbitrariness about the number; the purpose, public importance and size of programmes will differ. We believe that this rule could also be repealed. If annual reports show that there has been unreasonable use of a matching programme, that would be a legitimate matter for report by the Privacy Commissioner.

28 Ninthly, and finally, we raised in the issues paper the question of whether Inland Revenue should retain its current 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.[882] Those exemptions appear in section 101(5) and rule 6(3) of schedule 4 of the Privacy Act. Inland Revenue explained the need for the exemptions. Tax audits can take a long time; indeed, there is no time limit on a tax audit in a case of suspected evasion. A decision to take action may need longitudinal data collated via data matches over some years. Inland Revenue say that their governance processes are rigorous, and include regular reporting to the Office of the Privacy Commissioner.

29 We have no doubt that there are legitimate reasons to exempt Inland Revenue. The question is whether they should have blanket exemptions for all programmes whatever their purpose, or whether exemptions should be provided for in particular matching authorities where that is appropriate. We think the case is made for the latter but not the former, and so recommend. A majority of submitters to the issues paper agreed.

30 Should our recommendations for information sharing in appendix 1 be adopted, there will need to be power for an Order in Council to exempt Inland Revenue from the statutory requirement where that is appropriate for particular programmes.

882 Ibid, at [9.142]–[9.145].

LIST OF RECOMMENDATIONS ON INFORMATION MATCHING

31 These recommendations will only apply if the existing information matching regime is retained. (We have recommended that it be merged into the information sharing regime that we propose in appendix 1.)

RECOMMENDATION

R127 There should be a single definition of "information matching programme".

RECOMMENDATION

R128 The period of notice of adverse action provided for in section 103 should be 10 days, but with power in the Privacy Commissioner to reduce the period in appropriate cases.

RECOMMENDATION

R129 To the examples of "adverse action" in section 97 should be added decisions to impose a penalty and to recover a penalty or fine.

RECOMMENDATION

R130 Continuing programmes of information matching should have to be authorised, and operate, under Part 10 of the Privacy Act.

RECOMMENDATION

R131 Agencies seeking legislation to authorise an information matching programme should provide the Privacy Commissioner with a protocol describing the details of the programme; and the Privacy Commissioner should be able to require a Privacy Impact Assessment.

RECOMMENDATION

R132 There should no longer be a requirement of a five-yearly review by the Privacy Commissioner of every information matching provision, but the Commissioner should be able to conduct reviews as and when desirable.

RECOMMENDATION

R133 The government should be required to respond within six months of the presentation of a report on a review by the Privacy Commissioner of an information matching provision.

RECOMMENDATION

R134 The Privacy Commissioner should be able to report separately on information matching programmes rather than including such a report in his or her annual report.

RECOMMENDATION

R135 The information matching rules currently contained in Schedule 4 of the Privacy Act should be placed in the body of the Privacy Act, and the current rules 3 and 8 should be deleted.

RECOMMENDATION

R136 The current blanket exemptions for Inland Revenue contained in section 101(5) and rule 6(3) of schedule 4 should be repealed, but exemptions should be provided for in particular matching authorities where that is appropriate.

Appendix 3

The information privacy principles

PRIVACY ACT 1993, SECTION 6

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.

* [*See sections 27 to 29 below.*]

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 1 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.

(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.

PRIVACY ACT 1993, SECTIONS 27–29

27 Security, defence, international relations, etc

(1) An agency may refuse to disclose any information requested pursuant to principle 6 if the disclosure of the information would be likely—

(a) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by—

(i) the government of any other country or any agency of such a government; or

(ii) any international organisation; or

(c) to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or

(d) to endanger the safety of any individual.

(2) An agency may refuse to disclose any information requested pursuant to principle 6 if the disclosure of the information would be likely—

(a) to prejudice the security or defence of—

(i) the self-governing state of the Cook Islands; or

(ii) the self-governing state of Niue; or

(iii) Tokelau; or

(iv) the Ross Dependency; or

(b) to prejudice relations between any of the Governments of—

(i) New Zealand:

(ii) the self-governing state of the Cook Islands:

(iii) the self-governing state of Niue; or

(c) to prejudice the international relations of the Governments of—

(i) the self-governing state of the Cook Islands; or

(ii) the self-governing state of Niue.

28 Trade secrets

(1) Subject to subsection (2), an agency may refuse to disclose any information requested pursuant to principle 6 if the withholding of the information is necessary to protect information where the making available of the information—

(a) would disclose a trade secret; or

(b) would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information.

(2) Information may not be withheld under subsection (1) if, in the circumstances of the particular case, the withholding of that information is outweighed by other considerations which render it desirable, in the public interest, to make the information available.

29 Other reasons for refusal of requests

(1) An agency may refuse to disclose any information requested pursuant to principle 6 if—

(a) the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual; or

(b) the disclosure of the information or of information identifying the person who supplied it, being evaluative material, would breach an express or implied promise—

(i) which was made to the person who supplied the information; and

(ii) which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence; or

(c) after consultation undertaken (where practicable) by or on behalf of the agency with an individual's medical practitioner, the agency is satisfied that—

(i) the information relates to that individual; and

(ii) the disclosure of the information (being information that relates to the physical or mental health of the individual who requested it) would be likely to prejudice the physical or mental health of that individual; or

(d) in the case of an individual under the age of 16, the disclosure of that information would be contrary to that individual's interests; or

(e) the disclosure of that information (being information in respect of an individual who has been convicted of an offence or is or has been detained in custody) would be likely to prejudice the safe custody or the rehabilitation of that individual; or

(f) the disclosure of the information would breach legal professional privilege; or

(g) in the case of a request made to Radio New Zealand Limited or Television New Zealand Limited, the disclosure of the information would be likely to reveal the source of information of a bona fide news media journalist and either—

(i) the information is subject to an obligation of confidence; or

(ii) the disclosure of the information would be likely to prejudice the supply of similar information, or information from the same source; or

(h) the disclosure of the information, being information contained in material placed in any library or museum or archive, would breach a condition subject to which that material was so placed; or

(i) the disclosure of the information would constitute contempt of court or of the House of Representatives; or

(ia) the request is made by a defendant or a defendant's agent and is—

(i) for information that could be sought by the defendant under the Criminal Disclosure Act 2008; or

(ii) for information that could be sought by the defendant under that Act and that has been disclosed to, or withheld from, the defendant under that Act; or

(j) the request is frivolous or vexatious, or the information requested is trivial.

(2) An agency may refuse a request made pursuant to principle 6 if—

(a) the information requested is not readily retrievable; or

(b) the information requested does not exist or cannot be found; or

(c) the information requested is not held by the agency and the person dealing with the request has no grounds for believing that the information is either—

(i) held by another agency; or

(ii) connected more closely with the functions or activities of another agency.

(3) For the purposes of subsection (1)(b), the term **evaluative material** means evaluative or opinion material compiled solely—

(a) for the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates—

(i) for employment or for appointment to office; or

(ii) for promotion in employment or office or for continuance in employment or office; or

(iii) for removal from employment or office; or

(iv) for the awarding of contracts, awards, scholarships, honours, or other benefits; or

(b) for the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or

(c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property.

(4) In subsection (1)(c), **medical practitioner** means a health practitioner who is, or is deemed to be, registered with the Medical Council of New Zealand continued by section 114(1)(a) of the Health Practitioners Competence Assurance Act 2003 as a practitioner of the profession of medicine.

Appendix 4
List of submitters

The following organisations and individuals made submissions on the issues paper. Some individual submitters are not listed, to protect their privacy, but all submissions were greatly appreciated by the Law Commission.

Accident Compensation Corporation

Advertising Standards Authority

American Express International (NZ)

ANZ National Bank

Archives New Zealand

Association of Market Research Organisations New Zealand

Sir Bruce Slane, former Privacy Commissioner

Business New Zealand

Children's Commissioner

Commerce Commission

Dr David Erdos, University of Oxford

Judge David Harvey

Department of Building and Housing

Department of Corrections

Department of Internal Affairs

Department of Labour

Dun & Bradstreet New Zealand

Fairfax Media

Gehan Gunasekara, University of Auckland

Google

Government Communications Security Bureau

Gwilym Evans

Health and Disability Commissioner

Health Research Council

Human Rights Commission

IHC New Zealand

Inland Revenue

InternetNZ

Jenny Kelso

Kathryn Dalziel

Lindy Siegert

Malcolm Law

Marketing Association

Media Freedom Committee,
Commonwealth Press Union (New Zealand section)

Microsoft New Zealand

Ministry of Consumer Affairs

Ministry of Education

Ministry of Foreign Affairs and Trade

Ministry of Health

Ministry of Social Development

New Zealand Council of Trade Unions

New Zealand Customs Service

New Zealand Law Society

New Zealand Medical Association

New Zealand Police

New Zealand Post

New Zealand Press Council

New Zealand Qualifications Authority

New Zealand School Trustees Association

New Zealand Security Intelligence Service

New Zealand Transport Agency

Office of the Auditor-General

Office of the Clerk of the House of Representatives,
and Parliamentary Service (joint submission)

Office of the Ombudsmen

Office of the Privacy Commissioner

Professor Paul Roth, University of Otago

Plunket

Privacy Officers' Round Table

Recruitment and Consulting Services Association

Rob Dowler

Royden Hindle, former Chairperson, Human Rights Review Tribunal

Screen Production and Development Association of New Zealand

Shine* (safer homes in nz everyday)

Simpson Grierson Employment Law Group

SPARC: Sport & Recreation New Zealand

State Services Commission

Statistics New Zealand

Telecom Corporation of New Zealand

Television New Zealand and Radio New Zealand (joint submission)

Te Puni Kōkiri

Trade Me

Veda Advantage (NZ)

Wellington Community Law Centre

Westpac New Zealand

Women's Health Action Trust

YouthLaw Tino Rangatiratanga Taitamariki

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

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