

Part I

Preliminary Provisions

I

“Good, functional typography and design are invisible. Good design allows readers to concentrate their energy on substance rather than be distracted by format. A bad design remains a bad design, even though it may be redeemed to some extent by familiarity.”

- Law Commission, *The Format of Legislation*, 1993

“The Privacy Act’s accommodation of the concurrent needs for flexibility and certainty appears to have been bought at the price of simplicity.”

- Dr Paul Roth, preface to *Privacy Law and Practice*, July 1994

“The bill continues to cover the public and private sectors. There are exemptions and partial exemptions that are suitable now but it is intended that they be re-examined as time goes on. I am referring to the provisions on members of Parliament, the Parliamentary Service Commission, the Parliamentary Service, the news media, and the intelligence agencies. The bill gives power to the Privacy Commissioner to review the Act after 3 years, then at intervals of 5 years. The consequence of these reviews should be gradually to bring within the scope of the law those bodies I have listed, given the importance to them of the proper handling of personal information”.

- Hon Douglas Graham (Minister of Justice) on the Second Reading of the Privacy of Information Bill, April 1993

1.1 INTRODUCTION

1.1.1 Part I sets out preliminary provisions. Section 2 (interpretation) defines terms used throughout the Act. The definition of “agency” largely determines the scope of the Act’s application.

1.1.2 In this part of the report I comment upon sections 1-5 and where appropriate offer recommendations for amendment. Before moving to the section by section analysis I will address general style and drafting issues.

1.2 DRAFTING STYLE

Introduction

1.2.1 I hold the skills of the Parliamentary Counsel Office, which drafts New Zealand legislation, in high regard. The skill exercised in preparing such a ground breaking piece of legislation is evident throughout the Act. That the Act achieves the tasks set for it in a legally effective and appropriate manner is, in my mind, in no doubt. The provisions in the Act work very effectively by and large. It has not brought the problems predicted by long-standing opponents of indi-

vidual privacy rights. Credit in this respect is also due to the Justice and Law Reform Committee which studied the Privacy of Information Bill with such care and recommended significant amendments.

- 1.2.2 The Parliamentary Counsel Office and the select committee built upon established precedents which themselves had been prepared with great skill. The OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data were of particular importance on a conceptual and policy level. In terms of the structural and drafting issues, the Privacy Act 1988 (Commonwealth of Australia), the Official Information Act 1982 and the Ombudsmen Act 1975 were heavily drawn upon.
- 1.2.3 Nonetheless I am bound to say that the Act has not won universal acclaim for the simplicity of its drafting. In the course of the review, many people expressed to me a hope that aspects of the drafting and style of the Act could be simplified. It is appropriate that I give prominence to this issue at the outset of the Part by Part, section by section, discussion of the Act.
- 1.2.4 Lest there be any misunderstanding, I must add that criticism of the drafting or style of the Act is not universal, nor always deserved. Indeed, many regular users of the Act express a large measure of satisfaction. As agencies come to understand the law they often see it as appropriate, relatively straightforward and easy to use, and without significant shortcomings. The group of people who have the most difficulty with the Act are those who are not familiar with working with statutes.
- 1.2.5 Since the Privacy Act applies to such a wide range of agencies in the public and private sectors it is desirable that the Act be as “user friendly” to ordinary people as possible. If ordinary users of the Act within agencies are daunted from reading, and seeking to understand, the provisions of the Act there are risks that they will:
- continue with unfair information handling practices in a “business as usual” mode;
 - not base their decisions on the Act’s provisions but upon what other people tell them the Act requires - which may be wrong;
 - feel compelled to seek legal advice, with attendant costs, for what should be able to be readily ascertained by reading the legislation itself.
- 1.2.6 Various people have suggested to me that the Act could be rewritten in what they believe to be a clearer and more succinct style. It is conceivable that clearer structure and drafting could be achieved in a rewritten Act at comparable length to the present statute. However, I advise against attempting a major rewrite. A number of submissions emphasised the point, already apparent to me, that users of the Act have become familiar with the statutory structure and provisions and that wholesale change would provide an unwelcome disruption. It could also lead to uncertainty as to whether the changes are of substance or style.
- 1.2.7 However, there is scope to enhance the drafting and style of the Act while causing those familiar with the Act little disruption. In that light my recommendations on drafting style are premised upon there being no wholesale change to the section numbers presently in use. I have not lightly recommended splitting, switching, renumbering or reordering sections.
- General statutory format*
- 1.2.8 The format and presentation of New Zealand statutes is not too different from that in place at the time of the 1908 consolidation. Very little about our legislation appears “modern” whether one considers the page size, indentation, punctuation, use of capital letters, numbering, headings or a variety of other matters. The Privacy Act therefore has an unfamiliar “feel” about it for lay people

“The legislation is complex, lengthy and is not readily understood.”

- NZ BANKERS’ ASSOCIATION,
SUBMISSION S25

used to modern layouts, a range of font types, effective headings and such like in other documents they use. Anyone can achieve presentations in desktop publishing which, just a few years ago, were the preserve of typesetters and professional printers. The public, not unreasonably, now expect official publications to be presented in a clear and modern format from which they can easily locate the information that they need. This is not always the case with the Privacy Act.

- 1.2.9 While “ignorance of the law is no excuse” one can have sympathy for, say, a manager versed in business documents who possesses a copy of a statute yet cannot find the relevant passage or, when he or she does so, cannot understand it. Australia and Canada have modernised the presentation of their statutes beyond anything so far attempted here. The “office consolidations” produced in Canada even come with an index. The hypothetical business person would have a greater degree of confidence in using that legislation.
- 1.2.10 Big changes for the format, structure and style of New Zealand legislation have been proposed by the Law Commission and some aspects of these have been adopted, or are under study, by the Parliamentary Counsel.¹ I wish them well but turn to more modest reforms that I believe can be achieved in one statute, the Privacy Act. In making these recommendations I acknowledge that there is no “magic bullet” to turn a statute which has an old fashioned and complex look into a modern appearing, and simple to use, document.
- 1.2.11 Having ruled out recommendations which would significantly alter the familiar structure and numbering of sections, the format and style recommendations that I make are modest. However, within such constraints, I believe that changes could:
- rid the Act of some old fashioned aspects which discourage non-lawyers - the use of “shall”, Roman numerals, etc;
 - assist users to locate particular information within the text - through an enhanced analysis (list of contents) and marginal notes (headings);
 - direct users more effectively to other relevant statutes through reform of the section notes;
 - make some of the Act’s provisions easier to understand.
- 1.2.12 I approach the issues in the following order:
- adoption of Parliamentary Counsel Office changes in drafting style;
 - amendment to marginal notes;
 - consolidation of endnotes;
 - planning for a consolidated reprint;
 - noting other relevant recommendations.

Parliamentary Counsel Office changes in drafting style

- 1.2.13 The Parliamentary Counsel Office announced seventeen changes in its drafting style from 1 January 1997.² I have studied the changes and have concluded that six of them have some particular relevance to the Privacy Act. In Appendix E I have noted the six changes and added my own comments in respect of the Privacy Act. Briefly the proposed changes, and the relevance for the Privacy Act, are:

1. Dropping “of this Act” etc: This will make for shorter cross references within the Act as there would be scores, if not hundreds, of instances in the Privacy Act where the phrase “of this Act”, “of this section”, “of this subsection” or “of this principle” appear.

¹ See Law Commission, *The Format of Legislation*, 1993, and *Legislation Manual: Structure and Style*, 1996. I have adopted a more modern style in codes of practice than found in legislation. In doing so I have followed many of the Law Commission’s recommendations.

² See Parliamentary Counsel Office, *A Guide to Working with the Parliamentary Counsel Office*, September 1997.

2. Numbering parts in Arabic instead of Roman: The twelve Parts of the Act are currently identified by Roman numerals. The Second Schedule is similarly divided in this manner.
 3. Numbering schedules 1, 2 instead of First, Second: The Privacy Act’s eight schedules are currently labelled in the older manner.
 4. Alternatives for “shall” in appropriate cases: The Privacy Act uses “shall” in numerous instances. Each of the twelve information privacy principles uses the word “shall” at least once. Principle 7 uses “shall” five times. “Must” and “is to” are often satisfactory alternatives.
 5. Drop unnecessary “except as provided”, “subject to”, and “notwithstanding” formulations. These formulations appear in the Privacy Act at various places.
 6. Include further material in the analysis: The present analysis does not list the Act’s twelve information privacy principles, four public register privacy principles or eight schedules.
- 1.2.14 Of those changes, the most beneficial may be the simplest - listing the principles and schedules in the analysis. This will enhance the ability of users of the Act to locate relevant information. The other changes would be barely perceptible individually but taken together would mark an improvement in the style and appearance of the Act by:
- making it briefer in places - changes 1 and 5;
 - making the appearance more modern - changes 2, 3, 4, and 5;
 - making it more understandable to laypeople - changes 2, 4 and 5.
- 1.2.15 The Parliamentary Counsel Office has commenced a process of modernising and changing the drafting style in legislation. This is not something that can be achieved overnight and might not normally be attempted in an existing Act. I prefer that the unusual step be taken of introducing stylistic amendments throughout the text of the Privacy Act.³ If practicable I believe that the attempt should be made to adopt the modern format given the statute’s widespread applicability to a range of agencies.



RECOMMENDATION 1

The relevant changes in legislative drafting styles recently adopted by the Parliamentary Counsel Office should be applied throughout the Privacy Act.

Marginal notes and headings

- 1.2.16 Some of the marginal notes and headings have been found to be unhelpful, unduly technical or even misleading. The following changes are suggested:
- principle 9: “Agency not to keep personal information for longer than necessary” change to “Retention of personal information”;
 - section 7: “Savings” change to “Saving of effect of other laws” or “Effect of other laws on information privacy principles”;
 - section 27: “Security, defence, international relations, etc” change to “Security, international relations, maintenance of the law, safety, etc”;⁴
 - section 28: “Trade secrets” to “Trade secrets and prejudice to commercial position”;
 - section 42: “Documents” change to “Ways of making information available”;

³ My preference would be for the resultant reprint not to be cluttered with bold brackets highlighting changes which are purely stylistic. Otherwise some of the changes may increase rather than diminish clutter.

⁴ This change will be superseded if my recommendation to split the reasons for withholding into separate sections is adopted. See recommendation 47.

- section 45: “Precautions” change to “Precautions when giving access” or “Precautions concerning identity of requester or agent”;
- section 73: “Proceedings of Commissioner” change to “Parties to be informed of investigation”;
- section 95: “Disclosures of information, etc” change to “Disclosures of secret information, etc”;
- Part X: “Information matching” change to “Authorised information matching programmes”;⁵
- sections 100, 101 and 105: insert the word “authorised” before the phrase “information matching programme”;
- information matching rule 8: “Time limits” change to “Annual frequency of matching”.

- 1.2.17 The present heading of principle 9 has caused misunderstandings. The principle does not literally state that an agency is not to keep personal information for “longer than necessary”. Rather, it prohibits keeping information for “longer than is required for the purposes for which the information may lawfully be used”. A simple reference to “retention of personal information” in the heading may suffice to avoid confusion.
- 1.2.18 Section 7 needs to be found by any user of the Act who is to obtain a full appreciation of how the law works. Unfortunately, the special use of the word “savings” is not widely understood by non-lawyers. It is also used elsewhere in the Act (section 132). The alternatives of “saving of effect of other laws” or, preferably, “effect of other laws on information privacy principles” will direct the user of the Act to the relevance and importance of the provision more clearly.
- 1.2.19 The section 27 marginal note, taken directly from the Official Information Act, obscures the fact that the section includes two of the most important grounds for withholding information relating to the maintenance of the law and the endangering of the safety of any individual. Instead, attention is directed to security, defence and international relations, which are relevant to only a tiny proportion of access requests. The suggested change will downplay defence and emphasise the maintenance of the law and personal safety. The section 28 marginal note, trade secrets, presently describes only the first of alternative grounds for refusal of a request.
- 1.2.20 In sections 42 and 45 respectively, the marginal notes “documents” and “precautions” are taken from the Official Information Act which is a shorter statute dealing almost exclusively with access issues. In the wider scope of an information privacy law it is desirable to direct attention to the fact that the “documents” clause concerns the ways of making information available and “precautions” relates to precautions to be taken when giving access to verify the identity of a requester or agent.
- 1.2.21 The marginal note for section 73, “Proceedings of Commissioner”, is unfortunate since it conveys very little information and duplicates headings or subheadings used in Parts VIII and IX. A more informative note would be “Parties to be informed of investigation”. Similarly, the marginal note to section 95, “Disclosures of information, etc”, is too broadly stated for a general information privacy law. “Disclosures of secret information, etc” will better capture the effect of the section.
- 1.2.22 The heading to Part X should be changed to “*Authorised* information matching programmes”. Part X is not widely known or understood and confusion arises when agencies believe that Part X applies to them when in fact it does not. *Authorised* will make clear that the Part’s primary focus. Reference to *programmes* will emphasise the schemes being regulated.

⁵ A proposal to style “information matching” as “data matching” is canvassed at recommendation 119.

“There needs to be increased use of definitions as per Discussion Paper 1. As the Act has major impacts for, and is there to protect individuals and enhance privacy, the use of Plain English is imperative if they are to understand and use it. References to other Acts are couched in language which is often difficult for non-legal people to understand.”

- WELLINGTON CITY COUNCIL,
SUBMISSION WX5

- 1.2.23 Sections 100, 101 and 105 each concern “*authorised* information matching programmes” rather than the broader category of “information matching programmes”. The marginal notes should reflect this. Information matching rule 8 refers to “time limits” whereas it is more concerned with the frequency of matching.



RECOMMENDATION 2

The marginal notes and headings in the following principle, sections, Part and rule should be amended to make them more helpful, accurate and precise: principle 9; sections 7, 27, 28, 42, 45, 73, 95, 100, 101 and 105; Part X; information matching rule 8.

Section notes and endnotes

- 1.2.24 The published Act contains a variety of notes at the end of each section (referred to as section notes) and at the end of the Act (endnotes). The Law Commission has suggested more extensive use of statutory notes. The recent changes in drafting style adopted by the Parliamentary Counsel Office do not alter the use of notes. If the position changes it will be valuable to explore the inclusion of additional notes to enhance understanding of legislation.

- 1.2.25 However, in the absence of any general change I direct my remarks solely to existing notes. The only endnote is that the Act is administered in the Department of Justice (which, on reprinting, would show the *Ministry* of Justice). The existing section notes cross refer to other Acts on which the legislation is based. These are:

- the Privacy Commissioner Act 1991;
- the Privacy Act 1988 and the Data-matching Program (Assistance and Tax) Act 1990 (Australia);
- the Data Protection Act 1984 (UK); and
- the Ombudsmen Act 1975, the Human Rights Commission Act 1977, the Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987.

- 1.2.26 The Law Commission advises:

“Consider the practical value of the information before including a note. Do not allow a multitude of not very helpful references to some outdated statute to interrupt the flow and interfere with the appearance of an enactment. For example, it may be preferable to present a comparative table at the end of the Act rather than to give a note after each section.”⁶

- 1.2.27 There is definite value in having references to the official information legislation since this can direct users to secondary sources of interpretation of the sections and encourage consistent application of identical provisions. However, section notes do not convey full comparative information. For example, section 29 is followed with this endnote:

“cf. 1982, No.156, ss.18(c)(ii), (e), (g), (h), 27(1)(b) - (h), (2); 1987, No. 8, s.15(1); 1987, No. 174, ss.17(c)(ii), (e), (g), (h), 26(1)(b) - (h), (2).”

- 1.2.28 This information is of little use unless one can accurately match the paragraph and subparagraph references to paragraphs and subparagraphs within the section. I think it would be beneficial to move the section notes, or at least the Official Information Act references in Parts IV and V, to the end of the statute

⁶ Law Commission, *Legislation Manual: Structure and Style*, 1996, paragraph 121.

“Probably is room for improvement in wording of the Act to make it as easily understood as possible. This would enhance compliance. Also useful within an organisation to have people with specialist skills in this area to consult.”

- NZ ASSOCIATION OF
SOCIAL WORKERS AOTEAROA,
SUBMISSION WX4

in a comparative table or tables. Furthermore, unless one has some experience in using statutes the section notes simply appear to be “gobbledygook”. Only a user familiar with the legislative history of the statute, or who has access to a full set of statutes, will realise that the section note references are to the Official Information Act 1982, the Official Information Amendment Act 1987 and the Local Government Official Information and Meetings Act 1987. However, if the information were to be tabulated with the short title of each statute given it would be straightforward for all users of the Act to trace those helpful references.



RECOMMENDATION 3

The present section notes concerning the official information legislation should be presented in a comparative table at the end of the Act.

Consolidated reprint

- 1.2.29 It is expected that there will be an amendment bill to implement changes accepted by the Government. Those amendments, taken together with other amendments made since 1993, make the Privacy Act a suitable candidate for a consolidated reprint at an early date. A consolidated statute would capitalise upon any drafting and stylistic changes adopted. It would likely also be presented in a more modern design and typography as changes to this are currently under study by a working group.



RECOMMENDATION 4

The Parliamentary Counsel Office should be requested to arrange for a consolidated reprint of the Privacy Act following the implementation of reforms adopted as a result of this report.

Recommendations elsewhere in report

- 1.2.30 Throughout this report I have kept in mind the desirability of stylistic and drafting changes which will enhance the Act’s “user friendliness” for all users and especially for people unfamiliar with this Act or statutes generally.

SECTION BY SECTION DISCUSSION

1.3 SECTION 1 - Short title and commencement

Rapid commencement

- 1.3.1 The Act obtained the Royal Assent on 11 May 1993 and came into force less than two months later. This contrasts with the Official Information Act, which commenced precisely 10 years earlier, for which over six months was allowed between Royal Assent and commencement. It would have been valuable to have had longer to prepare for the commencement of the statute. A “breathing space” would have been desired by agencies and my office alike although I did at least have the advantage of having been Privacy Commissioner since 1992 - under the Privacy Commissioner Act 1991. Among the difficulties I faced was the coincidence of the commencement of the jurisdiction with the start of the financial year. With no transitional funding, the office had to expand from a staff of two, and then three, who had been involved in the advisory, policy and monitoring roles under the Privacy Commissioner Act, to provide a full enquiries and complaints service.
- 1.3.2 Despite severe strains upon the resources of a small and newly staffed office, considerable activity was undertaken to seek to assist in a smooth implementation of the Act. In the weeks between the assent and commencement a series of fact sheets were produced. Drafted with care, they remain in use years later. At the same time, a code of practice for the health sector was issued within a month of the commencement of the Act.

“Dunedin City Council believes that generally the Privacy Act is a workable piece of legislation which is in the best interests of all New Zealanders as long as it is approached and applied with common sense.”

- IN LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

- 1.3.3 I have little doubt that with a longer period for preparation the implementation may have been a little smoother - especially if the funding difficulty was avoided. Nonetheless, the Act's commencement was satisfactory, due in part, I expect, to the delayed enforceability of some provisions.

Delayed enforceability

- 1.3.4 Although the Privacy Act came into force on 1 July 1993,⁷ certain provisions did not become enforceable, or fully enforceable, until 1 July 1995⁸ or 1 July 1996⁹.
- 1.3.5 The delay in implementation of the enforceability of some of the principles was intended to give agencies a chance to prepare and, if necessary, to adjust their information handling practices. All the information privacy principles applied from the first day of the Act but enforceable remedies only became available immediately in respect of four of the principles. Delayed enforceability was designed to minimise the compliance cost impact as the new regime took force. I believe it was successful in that respect.

1.4 SECTION 2 - Interpretation

- 1.4.1 Section 2 is a key provision in the Act which assists in interpreting, and applying all the other provisions in the Act. The section sets out a series of definitions which are used to give a standard meaning to words or phrases that occur frequently in the Act. As the Law Commission's *Legislation Manual* explains, definitions contained in statutes can be used to delimit, extend, or restrict the meaning of a term in common usage.
- 1.4.2 A number of submissions were made that the answer to perceived problems of interpretation was to be found in creating new statutory definitions. While paying careful heed to all submissions, I approach such suggestions with considerable caution.
- 1.4.3 Sometimes the suggestions have been made in respect of relatively common English terms with which most users of the Act have little difficulty. The few users which do have difficulty sometimes insist upon fanciful or unlikely interpretations. Normal rules of statutory interpretation can easily cope with many such misunderstandings but a problem exists that many users of the Act are not familiar with the canons of interpretation. Such problems are not necessarily solved by inserting new statutory definitions which can bring a range of interpretational problems of their own.
- 1.4.4 More definitions mean a longer statute and the possibility of more rather than less complexity. On the question of creating new definitions I have tended to favour the *status quo* unless persuaded otherwise. However, if any significant problems of interpretation can be solved through simple new definitions then the opportunity should certainly be taken to adopt such change.
- 1.4.5 Section 2(1) contains 35 definitions and subsection (2) sets out a rule of interpretation. In the period since July 1993 there have been opportunities to consider and interpret many of these definitions by my office. A limited number of the terms have been considered by the Complaints Review Tribunal.
- 1.4.6 In the discussion paper I sought comment upon any of the defined terms, not simply those I had identified for particular attention. Very few of the definitions attracted comment and most have, I understand, worked perfectly ad-

⁷ With the exception of section 31.

⁸ See section 8(4).

⁹ See sections 9 and 79.

equately. This is not surprising since most of the definitions are straightforward and many have been used in other enactments such as the Official Information Act. However, in the paragraphs that follow I comment upon a number of the terms defined in section 2(1).

Agency

- 1.4.7 The definition of “agency” is particularly important as the information privacy principles are all expressed to apply to agencies. The definition starts out all-encompassing (a person or body of persons whether corporate or unincorporate and whether in the public sector or private sector) but continues with 13 exceptions. Accordingly, the series of exceptions are particularly important since they determine the overall scope of the Act.
- 1.4.8 Broad coverage is a prime feature of the New Zealand Privacy Act. Its seamless application to both public and private sectors means that most privacy issues are able to be reached by the Privacy Act. It also means that the legislation is little affected by demarcation disputes which accompany more narrowly based laws.
- 1.4.9 The definition of “agency” includes “any person whether in the public sector or in the private sector”. In theory, therefore, even a private individual who holds information about another person is subject to the Act. However, regard must also be had to section 56 which provides that the information privacy principles do not apply to the collection of, or holding by an individual of, personal information “solely or principally for the purposes of, or in connection with, that individual’s personal, family, or household affairs”.
- 1.4.10 As far as I am aware the definition of “agency” has caused few problems of interpretation in practice. Therefore, reviewing that provision is mainly directed towards considering whether the coverage of the Privacy Act should be narrowed (by creating new exceptions) or broadened (by narrowing or eliminating existing exceptions).¹⁰ In approaching this task I have been mindful of several considerations:
- broadening the exceptions will limit privacy rights and privacy protections whereas narrowing the exceptions may provide new rights for individuals in certain circumstances;
 - creating new exceptions would relieve some agencies of existing controls but such exceptions may create anomalies in the general “seamless” application of the Privacy Act and thereby increase complexity;
 - coverage of the Act was the subject of extensive public submission to, and intense scrutiny by, the original select committee.
- 1.4.11 Therefore, I have been persuaded against creating new exceptions which would limit individual rights and erode the Act’s coverage. On the other hand, I have not lightly recommended the elimination of some existing exceptions which were the subject of careful Parliamentary scrutiny. I have done this only in cases where experience, or further reflection, suggests they are no longer needed or are unnecessarily wide.
- 1.4.12 Bodies excepted from the definition of “agency” are placed completely outside the application of the privacy principles. It would be possible to avoid this by providing *partial* exemptions. Present examples include the exemption of courts in their “judicial functions” and, in section 57, intelligence organisations remain “agencies” but have a special exemption from certain principles. I see these partial exemptions as more satisfactory than total exemption.

¹⁰ See also the discussion of exemptions at paragraphs 6.10 - 6.13.

“The National Library has not had any major difficulties in working within the framework established by the Act. The experience of the last four years has been that a common-sense approach to working through the implications of the information privacy principles has proved a successful approach.”

- NATIONAL LIBRARY,
SUBMISSION S44

- Subparagraphs (b)(i) and (ii): Sovereign, Governor-General etc*
- 1.4.13 No issues have arisen, or been raised in consultation, in relation to the exceptions directed towards the Sovereign, the Governor-General and the Administrator of the Government.
- Subparagraph (b)(iii): House of Representatives*
- 1.4.14 No submissions were made to limit or remove this exception. However, I am aware that commentators have suggested that the Official Information Act 1982 should be reformed to grant rights of access in relation to the legislative branch of government.¹¹ The matter has also been the subject of study in Canada.¹² Proponents of such a change claim that it is an anomaly in relation to notions of “open government” that rights of access to information such as advisers’ reports do not exist in relation to, say, select committees.¹³ Although the Official Information Act would benefit from its own review it is unnecessary to directly enter into that debate here.
- 1.4.15 It may be timely to consider whether personal access rights under principle 6 (or indeed other aspects of the principles) should apply to the House of Representatives. Although the access rights in neither the Privacy Act nor the Official Information Act apply to the House of Representatives this does *not* mean that an individual will never be able to obtain personal information held about him or her by the House. There are already some procedural rules in Parliamentary Standing Orders and it may be that these are adequate to stand in the place of statutory rights.
- 1.4.16 Probably the main set of personal information at issue would be submissions and evidence to select committees. The general position is that written submissions remain confidential until, at the latest, they are publicly presented to the select committee at which time they become available.¹⁴ Evidence is almost invariably given in open hearing although it is possible to give private or secret evidence in closed session.¹⁵ Private evidence will be publicly available when a committee reports but secret evidence is only released by order of the House.¹⁶ Select committee reports themselves are published. However, prior to that time draft reports, and departmental advice to committees, are generally held confidentially within the select committee system although they must be shown to people who may be adversely affected by a finding.¹⁷
- 1.4.17 Individuals are free to obtain published select committee reports and to request copies of submissions and evidence where the committee has already reported. This will usually be made available unless classified as secret. However, there are a number of provisions in Parliamentary Standing Orders which provide for allegations concerning individuals to be put to those individuals, and for information to be released on request to a person whose reputation may be damaged.¹⁸ A witness is also given reasonable access to any information that the witness has produced to a committee.¹⁹

¹¹ Grant Liddell, “The Official Information Act 1982 and the Legislature” in Legal Research Foundation, *The Official Information Act*, 1997, pages 6-18.

¹² House of Commons, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, 1997, 8-9. The Standing Committee on Justice and Solicitor General recommended that the Access to Information Act, and the Privacy Act, cover both the Senate and House of Commons.

¹³ Although there is no such *right* of access, select committees are empowered to release information to assist in consideration of a matter. See *Standing Orders of the House of Representatives*, September 1996, Standing Order 241(2).

¹⁴ Standing Order 227.

¹⁵ See Standing Orders 219 to 223. Privacy or secrecy can only be accorded to evidence with *unanimous* consent of all members of the committee.

¹⁶ Standing Order 223(3).

¹⁷ Standing Order 245.

¹⁸ See Standing Orders 226 and 239.

¹⁹ Standing Order 238.

- 1.4.18 It is pleasing to note that provisions of the type described do exist in Standing Orders to allow some individuals to obtain access to information held about them. However, the key provision, Standing Order 239, is premised upon individuals being given access to information only where their “reputation may be seriously damaged by proceedings of a select committee”. This is based upon notions of defamation or natural justice rather than individual privacy. For example, an individual could not obtain, pursuant to Standing Order 239, access to evidence given in a Parliamentary inquiry that he or she was part of a group subject to a government scientific or medical experiment.
- 1.4.19 A principal difficulty with applying principle 6 and the right of access to Parliament relates to devising appropriate complaints or review mechanisms. In particular, it may seem constitutionally inappropriate to have the actions of Parliament reviewed by an external body since this could be seen to impinge on Parliamentary privilege and the notion of Parliamentary supremacy. It may be seen as objectionable in principle for legislation to refer to internal proceedings of Parliament as this may make them inherently justiciable.
- 1.4.20 I suggest if any of the information privacy principles were to be applied to the House of Representatives that the appropriate rule making vehicle might be Standing Orders, rather than statute. The appropriate review or complaints body would be the Speaker as the final interpreter of the House’s rules (subject to the House itself). If this matter is to be taken forward, it would be best for the initiative to come from Parliament itself and I do not propose any amendment to the Privacy Act.



RECOMMENDATION 5

An appropriate committee of Parliament should consider whether it is desirable to grant individuals access rights to information held about them by the House of Representatives or to adopt rules similar to any of the 12 information privacy principles.

- 1.4.21 It is worth noting that other rules and practices of the House of Representatives do exist to protect privacy. For instance the House has a rule that names of persons should not be used in questions unless they are strictly necessary to render the question intelligible.²⁰ Furthermore, the Speaker has endorsed a policy on access to personal information in petitions which expressly addresses the right to privacy of signatories to petitions²¹
- Subparagraph (b)(iv): Members of Parliament*
- 1.4.22 The exclusion of members of Parliament in their official capacities means that a complaint against an MP that personal information had been improperly obtained, used or disclosed publicly, could not be upheld if done in an official capacity. Generally I would not investigate such allegations.
- 1.4.23 In the context of the preceding discussion concerning the House of Representatives, I have emphasised the importance of the rights of access to information. In the context of MPs, the discussion in the last few years has tended to revolve around the justification for MPs bringing personal details of individuals into the public arena. Much of the debate has centred upon the exclusion of a citizen’s rights to sue an MP for *defamation* when Parliamentary privilege can be claimed. However, for most people the right to sue for defamation is an unlikely remedy due to the costs of litigation. Furthermore, it would provide no protection for the disclosure of truthful information which nonetheless ought to have remained private.

²⁰ Standing Order 371(1)(a).

²¹ Clerk’s Office Policy, “Access to Petitions”, endorsed by the Speaker on 22 June 1988.

- 1.4.24 While Parliamentary privilege is a necessary protection for MPs acting in the public interest to expose matters, often as a last resort on behalf of citizens, it is easy for other innocent individuals to have their personal details disclosed together with those of alleged wrongdoers. Furthermore, the exclusion of “a member of Parliament in his or her official capacity” is a much wider exclusion than the exemption that would apply as an incidence of Parliamentary privilege. It follows that it might therefore be possible to narrow the exemption while still absolutely preserving the aspects of the role of an MP pertaining to proceedings in Parliament.
- 1.4.25 It has been suggested to me that there are three capacities that may need to be considered:
- *Proceedings in Parliament* - this is the core area of Parliamentary Privilege. It includes speeches in the House and at select committees and a limited amount of administrative business closely connected with proceedings of the House - for example, lodging petitions, questions and bills. It would be inappropriate to have any legislative intrusion into this area (although Standing Orders could address such issues as was discussed above in relation to the House of Representatives itself).²²
 - *The capacity of a member* - this includes proceedings in Parliament but a great deal more besides. Members’ constituency work is not normally protected by Parliamentary privilege but it is work carried out in the capacity of a member of Parliament. Also included in this category are the caucus activities of members.
 - *Outside the capacity of a member* - this includes purely personal activities, of course, but it can include official activities undertaken in a capacity other than that of a member of Parliament. One obvious example of this is activities undertaken as a Minister where the Privacy Act already clearly applies. Some Ministerial work will be transacted in Parliament and so will form part of a proceedings in Parliament, but most does not so it is outside the capacity of a member. The issue was discussed in a recent report of the Privileges Committee.²³
- 1.4.26 When the opportunity has arisen, I have encouraged Parliament to adopt procedures which can adequately protect the personal information which comes into their possession. In my report on David Caygill’s Parliamentary Privilege Bill I offered support for the proposed “right of reply” whereby individuals could answer allegations made about them and have that answer placed in Hansard.²⁴ I am pleased to note that in 1996 the new Parliamentary Standing Orders introduced a procedure for any person (other than an MP) who has been referred to in Parliament in such a way as to be readily identifiable to apply to the Speaker for a response to be incorporated into the Parliamentary record.²⁵ This is akin to the proposed right of reply.
- 1.4.27 It seems to me that a few constitutional issues would arise in applying certain of the information privacy principles to MPs. I appreciate that the most vexed areas would be in relation to principle 11 governing disclosure. However, there would probably be few problems in, for example, applying information privacy principle 5 which would oblige MPs to take reasonable security safeguards in relation to their holdings of personal information. I believe that the Parliamentary Service Commission already offers some advice to MPs in relation to security of electorate officers, for example. Nor does it seem unreasonable that

²² See paragraphs 1.4.14 - 1.4.21.

²³ Report of the Privileges Committee (into a matter concerning Mr Rodney Hide MP), May 1998, I.15C, pages 7-9.

²⁴ See report of the Privacy Commissioner to the Minister of Justice on the Parliamentary Privilege Bill, 10 February 1995. The bill was carried over into a subsequent session of Parliament and remains there, now in the name of Jonathan Hunt MP.

²⁵ Standing Orders 164-167.

where MPs collect personal information from individuals that they make them aware of the sort of matters anticipated by principle 3. I also imagine that few MPs would have any problem with the notion that they be constrained from collecting personal information by unlawful or unfair means, as provided by principle 4.

- 1.4.28 One particular issue that I would like to see some movement on is the basis upon which personal information in an MP's constituency files, or client files, are held when an MP loses office. Constituents would not necessarily wish to see their files used as political ammunition nor simply see a complete halt to any ongoing dealings on their behalf with departments or Ministers.



RECOMMENDATION 6

An appropriate committee of Parliament should consider whether it is desirable to:

- (a) adopt any measures to encourage members of Parliament to apply, or follow, any of the 12 information privacy principle; or**
(b) provide that MPs in their official capacities are agencies for some purposes of the information privacy principles.

Subparagraphs (b)(v) and (vi): Parliamentary Service Commission and Parliamentary Service

- 1.4.29 The Parliamentary Service Commission is excluded from the definition of “agency” in total. The Parliamentary Service has a partial exemption but is an agency in relation to personal information held about an employee or former employee in his or her capacity as an employee.
- 1.4.30 The Parliamentary Service Commission and the Parliamentary Service are not subject to the Official Information Act. The Parliamentary Service Commission is an “organisation” for the purposes of the Ombudsmen Act but is specifically excluded from the same term in the Official Information Act.²⁶ Accordingly, the enactment of the Privacy Act constituted an advance in terms of access to information for employees. Although a small advance, I believe that it is an important one and that partial exemptions of that type are to be preferred over total exemptions wherever they can be accommodated.
- 1.4.31 The partial exemption for the Parliamentary Service means that the information privacy principles apply in respect of employee information. A significant effect of the limitation on the exemption is that employees can access personal information held by their employer. It does not appear that the principles apply to the Parliamentary Service in respect of the collection or holding of personal information about prospective employees.
- 1.4.32 I suggest that it is timely to reconsider the total exemption in (v) and the partial exemption in (vi). I have taken the position that exceptions should not continue without good reason. This differs from the approach taken in 1993 which was, by and large, to continue any approach taken in the official information legislation so as to avoid any inadvertent consequences.²⁷ The General Manager of the Parliamentary Service has indicated that there appear to be no compelling reasons why, in fulfilling its administrative functions, the Parliamentary Service should not be fully subject to the Act.²⁸ However, he was concerned

²⁶ See Ombudsmen Act 1975, First Schedule, Part II and Official Information Act 1982, section 2.

²⁷ The extension of access rights for employees of the Parliamentary Service is an unusual case where that conservative approach was not taken. When the Privacy of Information Bill was introduced it contained only the complete exemption for the Parliamentary Service Commission. During the examination of the Bill it became clear that the position of the Parliamentary Service needed to be clarified and the partial exemption offered a good compromise between total exemption, which would have denied employees any access rights, and no exemption at all.

²⁸ Letter General Manager, Parliamentary Service, to Office of the Privacy Commissioner, 14 July 1998.

that this be achieved in a way that does not impact upon the exemption for MPs in their official capacities. I incorporate that caveat in my recommendation. I have no specific suggestion for change in respect of the Parliamentary Service Commission but I recommend that the issue be further studied by officials to see if a narrowing of the exception is possible.

- 1.4.33 I note in passing that a recent review of the Australian Freedom of Information Act has recommended that Parliamentary departments should be subject to that access regime.²⁹ In New Zealand the Office of the Clerk, which I understand to be equivalent to an Australian Parliamentary department, is already subject to the Privacy Act.³⁰ The British Columbia Information and Privacy Commissioner has recently recommended that his province's information and privacy law should be extended to the administrative operation of the Legislative Assembly, including the Offices of the Speaker, the Clerk, the Legislative Comptroller, the Sergeant-at-Arms, Hansard and the Legislative Library.³¹



RECOMMENDATION 7

Consideration should be given to whether it is appropriate to replace the total exemption for the Parliamentary Service Commission in subparagraph (b)(v) of the definition of “agency” with a partial exemption.



RECOMMENDATION 8

The partial exemption for the Parliamentary Service in subparagraph (b)(vi) of the definition of “agency” should be repealed, or further restricted, if this can be achieved in a manner that does not impact upon the exemption in subparagraph (b)(iv).

Paragraph (b)(vii): Courts

- 1.4.34 Courts and tribunals were treated differently in the Privacy of Information Bill as introduced. Tribunals were excluded in relation to their judicial functions. Courts were excluded totally. The distinction was apparently carried forward from the Official Information Act and officials were unable to find a reason for it. The Select Committee removed the distinction and both courts and tribunals are excluded in relation to their judicial functions.
- 1.4.35 Most privacy, data protection or access laws carry an exclusion of some type in relation to the courts. For example, in a recent review of the Australian Freedom of Information Act the Law Reform Commission and Administrative Review Council concluded that it would continue to be appropriate that judicial documents be excluded from that Act.³² However, I am aware of one review which has recommended that courts should be subject to a Privacy Act notwithstanding that it would be inappropriate to apply an Act such as the Official Information Act. A Standing Committee of the House of Commons of Canada recommended that the Privacy Act cover the Supreme Court of Canada, the Federal Court of Canada and the Tax Court of Canada. It stated:

“The Committee believes that the Privacy Act should extend to all federal courts and administrative tribunals, since officers and employees of such institutions should enjoy the same rights to protect their privacy as are enjoyed by

²⁹ Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982, 1995*, recommendation 73.

³⁰ There is no exception applicable to the Office of the Clerk. Furthermore, it is expressly included in the definition of “organisation”.

³¹ Information and Privacy Commissioner, submission to the Four Year Review of the Freedom of Information and Protection of Privacy Act, February 1998, page 10.

³² Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982, 1995*, paragraph 117.

other federal officers and employees. However, the Committee agrees with the approach taken in most other jurisdictions and would not extend the Access to Information Act to cover the judicial branch of Government. Accordingly, the Federal Court, the Supreme Court of Canada and the Tax Court of Canada should continue to be excluded from the ambit of the Access to Information Act.”³³

- 1.4.36 The Canadian Committee referred expressly to the position of employees and their privacy. In New Zealand, the equivalent employees are employed by the Department for Courts and their personal information is therefore already protected and they have full rights of access and correction. To the extent that the judges might somehow become involved in employment matters, or hold, use or disclose information about their employees, they would probably fall outside the definition of a court acting “in relation to its judicial functions” and therefore would probably not be an “agency”.
- 1.4.37 Undoubtedly there are numerous personal sensitivities and privacy issues in relation to matters involving the courts. Courts obtain, often through legal compulsion, various personal information, much of it of some sensitivity. As an essential feature of our judicial processes evidence is given in open court and may be publicly reported. However, it is not clear that applying the information privacy principles to judicial processes would be of very much assistance in addressing privacy issues since there is also a well developed framework, directed towards regulating the issues and respecting the competing interests.
- 1.4.38 Traditionally the courts regulated their own procedures on such issues as the manner in which personal information (evidence) is obtained and produced before the court, how the accuracy of that information is verified, and the use to which the information may be put. Over the years the legislature has become more actively involved in the processes sometimes as a reaction to privacy concerns. One need only consider the issues of giving evidence in open court and its reporting. The common law position held that justice must be seen to be done and there were virtually no exceptions.³⁴ Parliament on the other hand has actively legislated to establish courts that generally hold private hearings (the Youth Court and the Family Court), to restrict the publication of evidence given in open court, to allow the public to be excluded from courts in a range of situations, for child witnesses and others to give their evidence in a manner that they cannot be seen by the accused and, recently, for secret witnesses to give evidence without being identified.
- 1.4.39 While I do not recommend change to the partial exemption, I do express the hope that the courts (and lawyers who appear before them) recognise that their processes have the potential to significantly intrude on privacy. Very frequently this is entirely appropriate and in the public interest. However, it may be acknowledged that courts have not always been alive to the sensitivities or the effect that their own rules of procedure can have. It may be argued that a failing on the part of the courts in a previous generation has led to Parliament to establish procedures to protect sensitivities surrounding divorce, rape, child abuse and the fears for the personal safety of witnesses. I do not recommend the existing partial exemption be altered.

Subparagraph (b)(viii): Tribunals

- 1.4.40 A submission was made on behalf of a body described as the “Tribunal of the

³³ Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, 1987, pages 8-9.

³⁴ The common law developed a very limited exception allowing for a closed court where justice could not otherwise be done, notably in blackmail cases.

Catholic Church for New Zealand”.³⁵ As the submission makes clear, this arose out of an actual complaint made to my office.³⁶ In that case, the agency claimed that it was a “tribunal” and therefore able to take the benefit of the exception. I formed the opinion that it was not and that the exception related to tribunals forming part of the New Zealand judicial system, that is statutory tribunals.

- 1.4.41 I am unpersuaded by the submission that the definition should be altered to apply to “private” tribunals. I do not believe that it was the original intention to exempt such bodies from the Act’s requirements. Nor do I think there is a case to change the substantive position. Private bodies are not subject to the same public scrutiny and accountability as statutory tribunals which help serve to ensure rights are protected. If any change were warranted it would be to put beyond doubt that the reference to “tribunal” means a statutory tribunal forming part of the New Zealand administrative or judicial structure.



RECOMMENDATION 9

Consideration should be given to including a definition of “tribunal” limited to statutory tribunals forming part of the New Zealand administrative or judicial structure.

- 1.4.42 Alternatively, my recommendation to allow proceedings on jurisdictional issues to be taken to the Complaints Review Tribunal will enable some of the borderline issues about whether a body is an “agency” to be determined quickly and authoritatively. Another case concerning the question of whether an agency is a “tribunal” has already arisen.³⁷

Subparagraph (b)(ix): Ombudsmen

- 1.4.43 Currently the Ombudsmen are excepted from the definition of “agency”. I am not satisfied that a complete exemption is necessary or desirable. There would seem to be three features of the Ombudsmen which might at first seem to warrant an exception. These are that:
- the Ombudsmen’s status as the review authority for complaints under the official information legislation puts them in a unique position making application of the principles inappropriate;
 - as Officers of Parliament, the Ombudsmen are in a similar position to the Parliamentary bodies exempted under subparagraphs (b)(iii) - (vi);
 - as a complaints body it would be undesirable for the Ombudsmen to be subject to complaints investigation by the Privacy Commissioner.
- 1.4.44 In my view, these do not support the exemption currently bestowed. It is not clear to me that the Ombudsmen’s responsibilities as the review authority for official information complaints require them to be exempted from the information privacy principles. At most this factor would support a partial exemption covering aspects of principle 6. However, I believe that the only important issue in this context is already met by section 55(d) of the Act excluding the application of principles 6 and 7 from correspondence to or from the Ombudsmen created in the course of an investigation under the Ombudsmen Act, Official Information Act or Local Government Official Information and Meetings Act.
- 1.4.45 I do not believe that the status as an Officer of Parliament should place the Ombudsmen outside the constraints applicable to other agencies subject to the information privacy principles. Certainly no exemption is provided to the

³⁵ Submission G7.

³⁶ The point at issue in the complaint was whether the individual concerned was entitled to have a *copy* of a document. The agency was willing to let the individual inspect the document but would not, as the Act requires, make the information available in the form requested by the individual through the production of a copy.

³⁷ See *Laing v Complaints Assessment Committee*, Complaints Review Tribunal, 5 June 1998, CRT decision No. 9/98.

Auditor-General or the Commissioner for the Environment. A learned commentator on Official Information Act matters has recently questioned the inconsistent exemption of officers of Parliament from access laws and advocated reform.³⁸

- 1.4.46 It seems inappropriate that those who deal with, or are employed by, the Ombudsmen have rights under the Human Rights Act but are arbitrarily denied rights under the Privacy Act. The privacy principles should apply for instance to security breaches and to unwarranted disclosures in the course of operations. It is anomalous that an employee of that office cannot have any independent review of the result of a personal access request even though that is quite properly granted in the employment contract.
- 1.4.47 There remains the point about an Ombudsman being subject to investigation on a complaint to the Privacy Commissioner. However, this does not in itself seem inappropriate. The Privacy Commissioner can, for example, be the subject of complaint to the Ombudsmen or the Human Rights Commission. The Race Relations Conciliator and the Human Rights Commission, amongst other complaints bodies, may be subject to investigation by the Privacy Commissioner and the Ombudsmen. Some overseas privacy laws expressly apply to ombudsmen.³⁹
- 1.4.48 As the Ombudsman model itself demonstrates so dramatically, the fact that an institution is subject to a complaints mechanism does not undermine public confidence in it but rather strengthens it. I have concluded that it would be desirable for the Ombudsmen to be subject to the information privacy principles.



RECOMMENDATION 10

Subparagraph (b)(ix) of the definition of “agency” should be repealed so that the Ombudsmen are considered to be an “agency” for the purposes of the Act.

Subparagraph (b)(xiii): News media

- 1.4.49 The Privacy of Information Bill did not provide an exemption for the news media. The bill was intended to implement the OECD guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data and those guidelines did not themselves have such an exemption. Indeed, it has, until recently, been unusual for international instruments on privacy to sanction, or promote, the exemption of the news media from some form of privacy or data protection controls. Accordingly, in Europe the relevant data protection laws normally apply to the news media. Clearly there is tension between expectations of privacy and the role of free news media. This tension exists whether or not there is a privacy law or a privacy law which applies to the news media. In human rights terms this might be seen as the tension between the right to freedom of expression and to protection of privacy.
- 1.4.50 In my capacity as an adviser to the select committee studying the Privacy of Information Bill I supported the creation of an exemption for the news media. It is not a total exemption but is nonetheless fairly extensive. The exemption applies to any “news medium” (a defined term) in its “news activities” (also defined). The exemption does not extend to a news medium in its capacity as, for example, an employer or a publisher of advertising.
- 1.4.51 The press lobbied strongly against the bill and members of the select committee commented adversely that they used their editorial pages to promote their

³⁸ Grant Liddell, “The Official Information Act 1982 and the Legislature” in Legal Research Foundation, *The Official Information Act*, 1997, page 15.

³⁹ See, for example the Freedom of Information and Protection of Privacy Act, British Columbia.

commercial interests. I considered then that an exemption for the news media was appropriate because:

- there was perceived to be a significant conflict between the privacy law and the legitimate activities of the news media and the exemption would ensure that the concerns about constraints on the news media, whether or not well founded, would not eventuate;
- although some suitable rules regarding the news media ought to be developed, the information privacy principles in unmodified form were probably not suitable and would not get to the heart of many news media privacy issues;
- broadcast news media were already subject to a privacy regime in the Broadcasting Act 1989. While there was no such statutory regime for the print media, the newspapers had not exhibited the privacy invasive practices witnessed in some overseas jurisdictions.

1.4.52 Despite statements by others to the contrary, I have not changed my views but I have carefully reconsidered my position in the light of my experience, the submissions made, including from the Commonwealth Press Union, and overseas trends.

1.4.53 A complete exemption for the news media is not the only approach that can be taken to reconciling the competing human rights and public interests. For example, it might be possible to:

- provide an exemption for those parts of the news media for which adequate alternative statutory, or self-regulatory, redress is available;
- provide a partial exemption whereby, say, principles 5, 8 and 12 apply to the news media but not the others;
- give a right of access to published information about oneself but not to unpublished information;⁴⁰
- apply the principles to the news media but consider whether any of them would need exceptions written into them to meet legitimate concerns;
- apply the principles in unmodified form and if problems eventuated to provide one off exemptions under section 54 or develop a code of practice under section 46;
- provide that the principles do not apply to the news media unless, and until, a code of practice is issued;
- apply a different set of principles to the news media.

1.4.54 I think that several of these options may be feasible. The only option I would wish to completely rule out is to apply the principles in unmodified form to the news media - I have no desire to see inappropriate constraints being placed on the news media. On the other hand, I do not favour any legislative move unless it is considered all prospects of satisfactory self-regulation have been exhausted.

1.4.55 Fourteen submissions were received in relation to the exemption for the news media. Seven considered that the exemption should be reconsidered⁴¹ while 7 thought it should be left alone.⁴²

1.4.56 Interestingly, the Europeans have now moved closer to the New Zealand situation with the European Directive on Data Protection anticipating the creation of new partial exemptions from data protection laws throughout all EU countries.⁴³ One issue that I have observed since 1993 has been the practice of

⁴⁰ Some newspapers already offer Internet search facilities which make some material readily retrievable. These could perhaps be linked to a correction statement facility as well.

⁴¹ Submissions G4, G6, G12, G15, G21, G22 and S2.

⁴² Submissions G10, G11, G17, G18, S18, S42 and S54.

⁴³ See EU Directive on Data Protection, articles 29 and 30(3). See also the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Recommendation 1/97 (Data protection law and the media), February 1997.

certain magazines to publish private details about individuals. Presently magazines have taken no action to establish any sort of self-regulation notwithstanding that many of them are published by companies which also publish newspapers subject to self-regulation through the Press Council. It was suggested to me in a consultation meeting that there may be a case to limit the exemption for the news media to those organisations which are subject to:

- a statutory process by which privacy complaints can be resolved - this would cover the broadcast media;
- agencies subject to a self-regulatory regime whereby privacy complaints could be addressed - those newspapers which participate in the Press Council scheme.

1.4.57 If the exemption were to be modified in this way thought would need to be given to judging the adequacy of alternative processes. Considerable work has been done in the EU to identify what might amount to an “adequate” self-regulatory regime for the protection of privacy.⁴⁴ The two main criteria are:

- the existence of an adequate set of rules or privacy standards by which agencies bind themselves;
- the existence of procedural/enforcement mechanisms which deliver:
 - a good level of compliance;
 - support and help to affected individuals;
 - appropriate redress.

1.4.58 The Broadcasting Act’s provisions would likely meet such requirements. A set of rules is promulgated through a code of practice under the Act and individuals may complain through the statutory processes and obtain compensation (albeit that the \$5,000 limit might be subject to criticism).

1.4.59 I doubt that the Press Council would presently meet the adequacy tests expected by the EU if these standards were ever to be applied. In my view, the Press Council would provide a suitable vehicle for adequate self-regulatory protection of privacy amongst the news media if it were to:

- adopt a code setting out the standards expected of the news media concerning respect for privacy; and
- provide for compensation or redress in cases where the code has been found to be breached and the individual has suffered as a result.

1.4.60 On the first point, the code of practice ratified by the UK Press Complaints Commission on 26 November 1997 would seem to provide a good basis upon which to model a New Zealand code.⁴⁵ In respect of compensation, the \$5,000 figure provided for in the Broadcasting Act would probably cover many such complaints. A mechanism for determining compensation could readily be devised and might involve, for example, the Press Council maintaining a panel of assessors from which the successful complainant could choose to have the matter referred.

1.4.61 I do not recommend any legislative change in respect of the current exclusion of the news media in their news activities from the definition of “agency” in section 2. However, there are important privacy issues and risks in relation to news media activities and I favour industry self-regulation with provision for remedies for affected individuals. In my opinion, an Industry Ombudsman scheme may work best at a low level and enable the Press Council to deal with unresolved complaints. It may have to see witnesses sometimes to determine

“I look forward to the Privacy Commissioner actually producing some good work because the forces of evil will mount against it. Once the Government has those principles in place it will realise that it has not yet heard anything from Wilson & Horton Ltd.”

- RT HON DAVID LANGE, THIRD
READING OF THE PRIVACY
COMMISSIONER BILL, 10 DECEMBER
1991

⁴⁴ See, for instance, Working Group on the Protection of Individuals with regard to the processing of Personal Data, “First Orientations on Transfers of Personal Information to Third Countries - Possible Ways forward in Assessing Adequacy”, June 1997 and European Commission DGXV, “Judging Industry Self-regulation: When does it make a Meaningful Contribution to the Level of Data Protection in a Third Country?”, January 1998.

⁴⁵ Press Complaints Commission, Code of Practice, 26 November 1997.

credibility. Alternatively, it could receive a report from an experienced journalist who would report to the Council. I am not of the opinion that the information privacy principles would work well for the news media and if privacy needs to be protected and no adequate self-regulatory code is developed with remedies for affected individuals, separate legislation would be more satisfactory than applying the Privacy Act to the issue.

- 1.4.62 The stridency of the reaction of the press to any criticism of their self regulation, their pathological opposition to privacy laws, unmatched by any other industry, their high error rate on reporting privacy issues and the personal attacks on my office will doubtless continue in their editorial columns. Editors feel vulnerable to laws which they see as making newsgathering more expensive as their own budgets are cut. Their pleas for a more active and systematic information authority for freedom of information have a sound basis for consideration. However their proprietors have been until now steadfast about the impossibility of drafting a code of practice or providing any recompense for breaches of their own standards - even with financial caps. My only interest is in respect of complaints about privacy and there is clearly a case for attempting standards such as the British Press Complaints Commission have demonstrated can be done or principles such as the Broadcasting Standards Authority has developed over the years. A recent indication of interest in establishing some standards on privacy by the new Chairman of the NZ Press Council is, in this respect, heartening.

Collect

- 1.4.63 The term “collect” is in common usage and easily understood. However, the Act delimits its meaning by stating that it “does not include receipt of unsolicited information.” The term is not generally defined in overseas privacy laws although some use and define the related terms of “solicit” or “obtain”.⁴⁶
- 1.4.64 Two submissions suggested that the definition of “collect” be amended. Submission G12 suggested that there can be confusion as to whether unsolicited information is covered by the Act. I take the view that the position is sufficiently plain - unsolicited information is not “collected” and therefore, principles 1 to 4 do not apply, but such information is “obtained” and therefore principles 5 to 12 will apply while the information is held by an agency.
- 1.4.65 Submission G8 suggested that the definition of “collect” should include the “generation of personal information by electronic or other means”. Although I do not discount the possibility that internally generated information may be “collected” in some circumstances, I expect that in most cases such information would be considered to be “obtained” but not “collected”. In any case, it does not seem likely that collection principles would have much relevance to the processes of internally generated information.
- 1.4.66 I am not otherwise aware of any significant difficulties with the term and do not recommend any change at this time.

Correct

- 1.4.67 The correction rights in principle 7 are derived from the Official Information Act but interestingly that Act has no definition of “correct”. As the Australian Privacy Act does not define the term either it appears that the definition was created especially for the Privacy of Information Bill as a derivation of the Australian principle 7. The definition makes it clear that “correct”, in relation to personal information, means to alter information by way of “correction, deletion, or addition”. In other words, correction does not solely take its ordinary meaning but includes, if there had otherwise been any doubt, the alteration of information by way of deletion or addition.

⁴⁶ See for instance, Privacy Act 1988 (Australia) and Data Protection Bill [HL] (UK).

- 1.4.68 It is correction by way of “deletion” which raises the most issues. In particular it raises the possibility of the use of the “correction” rights in principle 7 for the purposes of seeking deletion of information which may be objectionable to an individual not so much because of any inaccuracy but because it has been obtained without the individual’s consent. Typically the issue manifests itself in requests for deletion from mailing lists. This raises issues beyond the normal sphere of principle 7 but deletion in such circumstances is seen as a practical means of remedying breaches of principle 2, 3, 10 and 11. It also draws one into a debate, which I will not canvass in this context, as to whether it is appropriate to deal with marketing list issues on an “opt in” or “opt out” basis.
- 1.4.69 The correction right in principle 7 is derived from the “individual participation principle” in the OECD Guidelines. However, that does not actually use the term “correction” but instead states:

“An individual should have the right to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.”⁴⁷

- 1.4.70 Accordingly, the OECD equivalent to the New Zealand Act’s phrase “correct, delete or add” is “erase, rectify, complete or amend.” The European Union Directive introduces a new concept in its phrase “rectification, erasure or blocking”.⁴⁸ I discuss these issues further, in the context of principle 7 itself at paragraphs 2.9.8 - 2.9.15.⁴⁹ However, I simply observe at this point the relevance of the definition of “correction” to the issue.

Document

- 1.4.71 Submission G1 suggested that in defining “document” the Act should not be so specific in naming any particular technology. It pointed out that the definition refers, for instance, to “any tape-recorder” whereas these days a tape-recorder is only one device capable of recording voice. Sound and voice is frequently recorded digitally onto computers. I certainly agree that the definition needs to remain “technology neutral” so that in the future as new technologies emerge, and existing technologies converge, the definitions remain suitable.
- 1.4.72 The definition in the Act remains surprisingly appropriate given that its lineage traces back to 1980. It has withstood the ravages of technological change remarkably well. The definition of “document” is taken from the Official Information Act 1982 but in fact its roots go deeper than that. The Danks Committee recommended the present definition. In doing so it commented:

“This definition, which is the same as that in section 48G of the Evidence Act 1908 (as inserted by section 2 of the Evidence Amendment Act 1980) and in section 1A of the Commissions of Inquiry Act 1908 (as inserted by section 2 of the Commissions of Inquiry Amendment Act 1980), is intended to be as comprehensive as possible. Comparable definitions appear in clause 4 of the Australian Bill and in clause 3 of the Canadian Bill.”⁵⁰

- 1.4.73 I consider that it would be undesirable to unilaterally change the definition of “document” while a similar definition exists in several statutes. Although the definition of document remains sound I believe that a case can be made to

⁴⁷ OECD Guidelines, clause 13(d).

⁴⁸ European Union Directive on Data Protection, article 12(b).

⁴⁹ See also recommendation 25.

⁵⁰ Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981, page 61. The “Australian Bill” and “Canadian Bill” have since been enacted.

redefine it to either simplify its elements (by *removing* the examples of particular technology such as tape-recorders) or to make its illustrative value more relevant (by *adding* examples of modern technology, such as CD-Roms which did not exist in 1980). If change is made, it is desirable that this be done in conjunction with amendment to the definition of “document” in the official information and evidence statutes. It is therefore timely to note that the Law Commission has, in the course of its evidence law review, proposed the following new definition of “document”:

“**Document** means any record of information and includes:
 (a) anything on which there is writing or any image; and
 (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
 (c) anything from which sounds, images or writing can be reproduced, with or without the aid of anything else.”⁵¹



RECOMMENDATION 11

Consideration should be given to adopting a new definition of “document” in section 2 in conjunction with any redefinition of the term in the proposed Evidence Code.

Individual

1.4.74 The information privacy principles apply solely in relation to any “individual” as defined, that is “a natural person, other than a deceased natural person.” Although some submissions were made that it would be possible to state the definition more plainly⁵² or that it would be useful to define “natural person”⁵³ I consider that the definition is satisfactory. Clearly an “individual” is a living person - not a dead person.

1.4.75 However, the matter is complicated by the fact that section 46(6) redefines the term “individual” in relation to codes of practice concerning “health information”, as defined in section 46(7). The issues arising from this are discussed below in relation to section 46 at paragraphs 6.2.17 - 6.2.21.⁵⁴ If the recommendations to amend sections 46(6) and (7) are adopted, Parliamentary Counsel should consider whether there needs to be an amendment to “individual” in section 2 as well. Otherwise if more extensive use is made of section notes in future, it may be useful to provide a cross reference between the two definitions.

Information privacy principle

1.4.76 The definition of “information privacy principle” is quite plain and does not, in my view, require change. However, I record that, for a full understanding of how the Act works, it is necessary to be aware that section 53 of the Act, which outlines the effect of a code of practice, means that in some instances references in sections of the Act to an “information privacy principle” need to be read as references to a rule in an applicable code of practice.

Permanent resident of New Zealand

1.4.77 The term “permanent resident of New Zealand” appears only in section 34 and therefore it may be advantageous to users of the Act to move the definition from section 2 into that section. However, I have separately recommended that the standing requirements in section 34 should be repealed or amended.⁵⁵ If

⁵¹ The Law Commission, *Draft Evidence Code*, March 1998.

⁵² Submission G1.

⁵³ Submission G12.

⁵⁴ See also recommendation 75.

⁵⁵ See recommendation 61.

the section is repealed this definition should also be repealed. If section 34 is amended, or some distinction continues to be made between citizens, permanent residents and others, there may continue to be a need for this definition.

Personal information

- 1.4.78 “Personal information” is defined consistently with the definition of “personal data” in the OECD Guidelines.⁵⁶ The definition is a derivation of one that appeared in the Official Information Act 1982. It is a term that is central to the Privacy Act’s operation and is satisfactory for that purpose.
- 1.4.79 The only complication in relation to the definition is the phrase that states that the term “includes information contained in any register of deaths that is maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995, or any former Act”. This makes it clear that information about deceased persons is encompassed within the term in relation to information held on the deaths register. The main reasons for making this clear relate to the application of the:
- public register controls in Part VII of the Act; and
 - the information matching controls in Part X of the Act.⁵⁷
- 1.4.80 However, a complication arises because the definition encompasses information “contained in” the register of deaths leaving open the position of information sourced from, but no longer contained in, the register (that is, after the information has left the register and is in the hands of another person). That of itself is not problematic in relation to obligations on the Registrar of Deaths under the public register privacy principles. However, it might call into question the effectiveness of public register privacy principle 2 as it applies to *other* persons using information sourced from the deaths register. It might also lead to interpretational complications if an information matching programme were to be authorised involving the register of deaths.



RECOMMENDATION 12

Consideration should be given to amending the definition of “personal information” to clarify the position of information sourced from, but not contained in, the register of deaths.

Public register

- 1.4.81 The definition of “public register” is discussed in relation to section 58 at paragraphs 7.2.4 - 7.2.11.

Public sector agency

- 1.4.82 In reviewing the definitions I have given consideration to any opportunity to “unclutter” a key interpretation section in the Act. In some instances the interpretation provisions may be over-elaborate due to complexities inherited from other statutes. Accordingly, I have sought out opportunities to delete or combine definitions and to remove complexities.
- 1.4.83 The definition of “public sector agency” appeared to offer possibilities in that regard. Although the definition itself is not taken from the official information legislation the concept, and most of the constituent parts of the definition, are derived from the two official information statutes and the Ombudsmen Act. The current definition is perfectly workable and I have no particular wish to alter the position *in substance*. However, I consider that it may be possible to

⁵⁶ Article 1 defines personal data to mean “any information relating to an identified or identifiable individual”.

⁵⁷ The Privacy Commissioner Act 1991, and the Privacy Act 1993 at the time of its enactment, provided for information matching involving the deaths register. Although that provision was dropped at the time of the consolidation exercise involved in enacting the Births, Deaths and Marriages Registration Act 1995, it is anticipated that information matching involving the deaths register may again be authorised at some future time.

more briefly express the definition by combining and simplifying the constituent parts (by which I mean the definitions of department, local authority, Minister and organisation).

1.4.84 Accordingly, I considered the following possible definition:

Public sector agency:

(a) means an agency that is:

- i a Minister;
- ii a Government department named in Part I of the First Schedule to the Ombudsmen Act 1975;
- iii an organisation named in Part II of the First Schedule to the Ombudsmen Act 1975 or the First Schedule to the Official Information Act 1982, or both;
- iv a local authority or public body named or specified in the First Schedule to the Local Government Official Information and Meetings Act 1987 including any committee or subcommittee which the local authority is empowered to appoint, and a committee of the whole authority; and

(b) includes:

- i the Office of the Clerk of the House of Representatives;
- ii an intelligence organisation; and
- iii any agency that is an unincorporated body (being a board, council, committee or other body) established in accordance with the provisions of any enactment or by any such public sector agency for the purpose of assisting or advising, or performing functions connected with, any public sector agency within the meaning of paragraph (a) or (b).

1.4.85 If this definition is adopted then it may be possible also to repeal some, or all, of the definitions of department, organisation, and local authority. The need for some of those other definitions is, in any case, diminished by some of the other recommendations I make.⁵⁸ I suggest leaving the definition of “Minister” because that will continue to be needed notwithstanding other recommendations I am making. Where it is necessary to refer to a term which is no longer defined, it would be possible to, for example, refer to “a local authority within the meaning of paragraph (a)(iv) of the definition of public sector agency”.

1.4.86 However, if my recommendation to amend the definition of “public sector agency”, and to repeal the constituent definitions, is not accepted I nonetheless suggest that consideration be given to simplifying aspects of these five definitions and the clause I have tentatively set out above may suggest a way to do this.⁵⁹



RECOMMENDATION 13

Consideration should be given to redefining or recasting “public sector agency”, “Minister”, “department”, “organisation” and “local authority”.

1.4.87 Consideration should also be given to defining as a class those agencies that are not public sector agencies. The obvious title would be “private sector agency”. A suitable definition might be:

Private sector agency means an agency which is not a public sector agency.

⁵⁸ Such as recommendations 34, 70, 115 and 147.

⁵⁹ For example, “local authority” could be defined somewhat more simply than at present through the formulation set out at paragraph (a)(iv) of the proposed definition of public sector agency.

- 1.4.88 The usefulness of this term lies in the fact that it could be used to replace various references in the Act to “any agency that is not a public sector agency”. Such references can be found in sections 3, 35 and 46. Section 35 concerning the making of charges will particularly benefit from the resultant simplification.



RECOMMENDATION 14

Consideration should be given to enacting a definition of “private sector agency”.

Publicly available information and publicly available publication

- 1.4.89 “Publicly available information” is a term that is used in several of the exceptions to the information privacy principles.⁶⁰ The term is not as wide as might first be thought as the definition makes it clear that it means personal information that is contained in a “publicly available publication” which is defined to mean:

“a magazine, book, newspaper, or other publication that is or will be generally available to members of the public; and includes a public register”.

- 1.4.90 The definition of publicly available publication is derived from the definition of “generally available publication” in the Australian Privacy Act 1988 although that Act does not use the term as the basis of an exception in the way that the New Zealand Act does. The Australian definition of “generally available publication” is expressed to mean “a magazine, book, newspaper or other publication that is or will be generally available to members of the public”.⁶¹
- 1.4.91 The inclusion of exceptions related to publicly available information may be argued to contribute to the workability of the Privacy Act since it might be difficult to apply privacy principles to personal information in publications where there is, by definition, no control over how they are used and disclosed because of their “public availability”.
- 1.4.92 Whether something is a “publication” that “is or will be generally available to members of the public” is not always clear. The Act deems public registers to be included in the definition but there is less certainty with regard to such materials as:
- statutory registers that are not “public registers” listed in the Second Schedule;
 - official reports to which the public is entitled but which have not been published;
 - material made available on an Internet site.
- 1.4.93 I merely mention these areas of possible interpretational difficulty. I await a suitable case to form an opinion on such questions, which can, in turn, be subject to definitive interpretation by the Tribunal if necessary.
- 1.4.94 There are some other types of information which, in other contexts have been described as being “in the public domain” (this term is not used, and is generally inappropriate, in respect of information privacy legislation) such as information that has been broadcast. For instance, a tape recording made by an individual of a radio broadcast would not constitute “publicly available information” in terms of the definition (although a cassette tape on sale commercially might constitute a “publicly available publication”). Another non-traditional type of publication would be an “electronic book” supplied on a disk or CD-Rom. Where such an electronic publication is made generally available to members of the public I have little doubt that it would be considered a “pub-

⁶⁰ See information privacy principles 2(2)(a), 10(a) and 11(b).

⁶¹ Privacy Act 1988 (Australia), section 6.

licly available publication” (although the issue has yet to be tested in a complaint).

- 1.4.95 None of the examples that I have just mentioned warrant, in my view, amending the definitions. However, there is one circumstance in which I believe action is warranted since otherwise an anomaly may exist. This relates to the inclusion of “public registers” in the definition. “Public register” is defined in sections 2 and 58 essentially to mean a register, roll, list or other document maintained pursuant to a public register provision listed in the Second Schedule. In other words, only some registers, rolls etc maintained pursuant to statutory provisions are “public registers” for the purposes of the Act. Accordingly, it appears to me those other registers or rolls etc will only be “publicly available publications” if they can be characterised as falling within the first part of the definition, that is being a “magazine, book, newspaper, or other publication”. Some registers are actually maintained in books. Some others are, from time to time, published in book form.⁶² Accordingly, 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.
- 1.4.96 Any expansion of the definition of publicly available publication will, in effect, diminish the application of the privacy principles through the widening of the exceptions. However, that may be appropriate if one accepts the basic premise that an exception is necessary.
- 1.4.97 In recommendation 96 I have suggested that a process be undertaken to bring statutory registers open to public search into the list in the Second Schedule. As that work advances the extent, and effect, of any anomaly is diminished. That of itself is an appropriate response and that therefore it is unnecessary to broaden the definition of “publicly available publication” to include other registers maintained pursuant to law which are open to public search.

Statutory officer

- 1.4.98 The term “statutory officer” is only used in section 3 and it seems to make more sense that the definition should be placed in that section. This will ensure that people using section 3 are aware of the defined term while uncluttering section 2 for definitions of general application.



RECOMMENDATION 15

The definition of “statutory officer” should be moved from section 2(1) into section 3.

Working day

- 1.4.99 “Working day” has an importance in relation to those places in the Act where time periods are expressed. For example, section 40 makes it clear that a decision on an information privacy request is to be made as soon as reasonably practicable and in any case “not later than 20 working days” after the day on which it is received. The definition differs from that contained in the Interpretation Bill now before Parliament since it excludes the period between 25 December and 15 January.
- 1.4.100 The only context in which I can recall any problems being ascribed to the definition in section 2 is in relation to information matching under Part X, which has its own additional set of definitions in section 97. Unfortunately, on occasion people working with Part X have failed to familiarise themselves with the other Parts of the Act including the definition of “working day”. The defi-

⁶² The register of medical practitioners, for example, is not currently listed as a public register but is open to public search and, from time to time, is published as a supplement to the *New Zealand Gazette*.

inition of working day applies throughout the Act, including Part X. Agencies involved with information matching may need to make themselves more familiar with section 2 but I recommend no change to the Act in this respect.

New definitions

- 1.4.101 In submissions, suggestions were variously made as to the merits of new definitions for:
- public interest;
 - indexed or organised;
 - search reference;
 - electronic transmission;
 - statutory register;
 - disclosure;
 - use;
 - obtain;
 - reasonable;
 - research purposes.
- 1.4.102 I considered the merits of each of these suggestions and others. I have suggested elsewhere that consideration be given to defining “tribunal” and “trade secret”.⁶³ However, “use” is the only other term which I consider may warrant definition at this stage.⁶⁴

Use

- 1.4.103 An issue has arisen overseas as to whether “browsing” constitutes a “use” of information under a privacy or data protection law. An English case suggests that simply reading personal information, but not to employ that information for a purpose, may not constitute “use”.⁶⁵ In that case it could be shown that a police officer had checked a confidential police database for details of debtors being investigated by his friend but it could not be proved that the information had indeed been passed on or actually put to a use. The court treated the accessing of the computer records as a pre-requisite to use rather than use itself.
- 1.4.104 The Data Protection Bill presently before the UK Parliament defines “processing” of personal data to include “retrieval, consultation or use of the data”.⁶⁶ It would appear that if browsing of data does not constitute “use” then it will almost certainly constitute “retrieval” or “consultation”. It may be that this is the legislative response to the problem thrown up by the earlier case.
- 1.4.105 I too had to form a view on the meaning of the “use” in an information privacy principle 8 case where an agency stored and retrieved information but nothing else had apparently happened. In the circumstances of that case, I concluded that in order to show that some usage had occurred, the retrieval would need to have been followed by some action. In that case, the inaccurate information was simply deleted.⁶⁷ However, browsing is not really an issue in respect of the way “use” is used in principle 8. Browsing is essentially a problem involving authorised users of a database accessing information they have no business in seeing or using. It is therefore more of an issue in respect of principles 5 and 10 than principle 8 and the issue has not yet been tested in New Zealand under those other principles.
- 1.4.106 Browsing of sensitive personal information by employees of the Internal Revenue Service caused a scandal in the USA in 1993/94 and in subsequent years. Internal audits in 1997 confirmed a worrying level of browsing by IRS employees of confidential tax files of notable people and others.⁶⁸ As a result the IRS

⁶³ See recommendations 9 and 50.

⁶⁴ The Privacy of Information Bill did define “use” but the definition was omitted by the Select Committee. However, the original definition would not have addressed the issue discussed here.

⁶⁵ *R v Brown* [1996] 1 All ER 545.

⁶⁶ Data Protection Bill [HL] (UK), 4 June 1998 version, section 1(1), paragraph (b) of definition of “processing”.

⁶⁷ Case note 9257.

⁶⁸ Reportedly 1515 IRS workers had been investigated for browsing through tax files. See “Surprise? Browsing Tax Files still a Problem at IRS” 17/8 *Privacy Times*, 17 April 1997, page 3.

prosecuted some staff. However, the US Federal Court of Appeals held in one important case that an IRS employee could not be convicted because he merely looked at confidential tax data for unauthorised purposes but was never proven to *use* the information as part of a fraudulent scheme. A report of the case⁶⁹ suggested that the defendant was a member of a white supremacist group who regularly snooped through the IRS’s computerised integrated data retrieval system. Targets included tax returns of members of a political campaign, the tax return of an assistant district attorney (who had been prosecuting the defendant’s father on an unrelated charge) and his wife, the tax return of a city councillor’s campaign committee (who had defeated the defendant in a council election), the tax return of his brother’s instructor, and the tax return of a woman the defendant had dated a few times, amongst others. The actions, although reprehensible, could at most lead to a dismissal of the employee but not the prosecutions that the IRS had laid.

- 1.4.107 The US decision prompted an IRS Commissioner to ask Congress for legislative amendments to make such browsing a felony. As a result the Taxpayer Browsing Protection Act was enacted into law on 5 August 1997. That law makes it a misdemeanour for an IRS employee to review tax records without authorisation. The law also creates a civil remedy based on an unauthorised inspection of tax return information and requires the IRS to notify taxpayers when an IRS employee is indicted or otherwise charged for improper browsing of their information.⁷⁰
- 1.4.108 Browsing of taxpayer files by staff has also been uncovered at the Australian Tax Office. Successful prosecutions have been brought under the ‘computer crime’ provisions in the Commonwealth Crimes Act.⁷¹ There are no equivalent computer-related offences in the New Zealand Crimes Act as discussed at paragraphs 12.16.13 - 12.16.16.
- 1.4.109 It seems to me that the unauthorised retrieval or consultation of personal information in the circumstances known to have occurred in the UK, USA and Australian cases is the proper subject of the information privacy principles. Such browsing could easily be as serious as some other incidental or administrative use of information which already falls within the scope of the principles. It appears from some of the reports of browsing that the issue often concerns a matter of proof. The authorities have been able to prove that an employee consulted certain confidential records for which they had no proper purpose but could not show that the employee actually disclosed the information to someone else or used it in some way.
- 1.4.110 The matter could be taken forward in several ways. One might be to define “use” to include the elements of browsing. A suitable definition might be as follows:

“use, in relation to information, includes retrieval, consultation or use of information.

There was considerable interest in submissions in the proposal to define “use” to encompass browsing with responses, mixed, but generally favouring the issue being addressed.⁷²

⁶⁹ See “Unauthorised Access to IRS Files not a Felony, Court says”, 17/6 *Privacy Times*, 19 March 1997, 1-2. A Tennessee jury on similar grounds acquitted as IRS employee caught snooping through the records of such celebrities as Lucille Ball, Elvis Presley, Elizabeth Taylor and Tom Cruise (see *Privacy Times*, 17 April 1997).

⁷⁰ The report on the new Act is taken from “Legislative Round-up” 5/1 *Privacy & American Business*, March/April 1998, 14.

⁷¹ See “Raiser v Slodac (1995)” in 5 *Privacy Law & Policy Reporter* (1998) 13.

⁷² See submissions K11-K14, K18, K19, K21, K24, K28, K29, S13, S19 and S42.

“To extend the meaning of ‘use’ to incorporate ‘browsing’ would potentially be to penalise an action which has no recognisable consequences.”

- NZ EMPLOYERS

FEDERATION, SUBMISSION K14

- 1.4.111 An alternative would be to tackle the issue of browsing in the relevant principles. Accordingly, the issue could be tackled in, say, principle 5, but principles 8 and 10 could be left as they are. I recommend that further consideration should be given to defining the term “use” in section 2. However, my principal recommendation is to take the matter up in principle 5 and I discuss this elsewhere.⁷³



RECOMMENDATION 16

Consideration should be given to the desirability of enacting a definition of “use” which will encompass the retrieval, consultation or use of information.

Section 2(2)

- 1.4.112 Subsection (2) is an 89 word sentence provided “for the avoidance of doubt”. It has been criticised for being lengthy and convoluted. In fact, with a little study, the ideas conveyed in the provision do not seem particularly complex. However, apparent complexity is compounded by the fact that it links to a subparagraph in the definition of “agency” which is, itself, expressed in a perplexing way (a commission of inquiry, etc, “appointed, pursuant to, and not by, any provision of an Act...”).
- 1.4.113 The provision is included out of an abundance of caution. Given my desire that the statute be user-friendly for lay people, I am concerned to have such drafting in the key interpretation section. I recommend that the provision be redrafted in a plainer fashion if possible. It should be noted that part of the phraseology is also used in section 55(c) and there is a need for consistency.



RECOMMENDATION 17

Section 2(2) should be replaced with a more concise provision.

1.5 SECTION 3 - Information held by agency

- 1.5.1 Section 3 sets out the circumstances where information is deemed to be held by an agency. Information held in an official, employment, or membership capacity is deemed to be held by the agency itself, as is information held by another agency where that agency is linked by an agency or bailment relationship, or a contractor relationship limited to data processing only, and where it does not use or disclose the information for its own purposes.
- 1.5.2 I have already noted that “statutory officer” is used in this section but not elsewhere in the Act. I have therefore made the suggestion that the definition be removed into section 3 for convenience of users. “Statutory officer” is a term derived from the Official Information Act 1982 and has been interpreted in that context. It has not yet been the subject of consideration by the Complaints Review Tribunal in the context of the Privacy Act.

1.6 SECTION 4 - Actions of, and disclosure of information to, staff of agency, etc.

- 1.6.1 This section provides that for the purposes of the Act agencies are responsible for the actions of, or information disclosed to, their employees. Similarly, section 126(1) provides that for the purposes of the Act employee’s actions are to be treated as the employer’s - whether or not the latter knew or approved of them. However, in any proceedings under the Act the employer will have a defence under section 126(4) if he or she took “such steps as were reasonably practicable” to prevent the employee taking that action or actions of that type.
- 1.6.2 It is unfortunate that it is necessary for employers and employees to locate

⁷³ See recommendation 23.

“Sections 3 and 4, together with section 126 do not, in practice, appear to have caused any particular difficulty, although situated at opposite ends of the statute. There could, however, be an inherent difficulty for some smaller employers in grasping the initial fact that they are covered by the term ‘agency’. This is something which requires education rather than legislative tinkering.”

- NZ EMPLOYERS FEDERATION,
SUBMISSION G10

sections in opposite ends of the statute to obtain the complete picture. However, I believe that an employer who reads both sections will obtain a relatively plain message as to the combined effect of the provisions. I have earlier concluded that it will be undesirable to switch the order of sections or generally change the Act's existing numbering system and structure. Accordingly, while the position is not ideal I do not recommend change. However, if, at some stage, greater use is made of endnotes in statutes I suggest that a cross-reference be provided.

1.7 SECTION 5 - Act to bind the Crown

- 1.7.1 Clause 27 of the Interpretation Bill, presently before Parliament, provides that no enactment binds the Crown unless it expressly provides that the Crown is bound. That clause re-enacts section 5(k) of the Acts Interpretation Act 1924. If the Law Commission's recommendation to reverse that statutory presumption ultimately prevails it may no longer be necessary to have a provision such as section 5. However, subject to any need to reconsider the matter if the Interpretation Bill is amended, there is no reason to alter section 5.