

Part II

II

Information Privacy Principles

57

“With regard to the rest of the Privacy Act 1993, our members do not report any major difficulties and have found that compliance is largely a matter of good business practice.”

- Insurance Council of New Zealand, submission L9

“We understand that a number of people have suggested that changing the expression and ordering of the information privacy principles at this point is unnecessary given their broad general acceptance in the community. We submit that the complexity, repetitiveness, and illogical ordering of some of the principles and their associated provisions are major barriers to the understanding of the Act and urge that consideration be given to a major reorganisation exercise.”

- NZ Law Society Privacy Working Group, submission K29

“A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these guidelines or where re-export of such data would circumvent its domestic privacy legislation”.

- OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, clause 17

2.1 INTRODUCTION

2.1.1 Part II includes 6 sections:

- *section 6*: the principles themselves;
- *section 7*: which saves the effect of certain other enactments;
- *section 8*: which sets out the application of the principles to information collected, obtained or held before or after the Act’s commencement;
- *section 9*: postponing the application of the disclosure principle to lists used for direct marketing to mid-1996;
- *section 10*: applying the principles to certain information held overseas;
- *section 11*: governing the enforceability of the principles.

2.1.2 The information privacy principles are at the heart of the Privacy Act. In other countries it is common for privacy or data protection acts to contain sets of principles. It has been found to be an appropriate means of translating the concepts of information privacy into a legally effective form.

“The Privacy Act has not been a burden for many agencies. Public complaints about compliance costs may be exaggerated. The generally non-prescriptive nature of the legislation confers advantages in comparison with overseas models.”

- NZ LAW SOCIETY PRIVACY WORKING GROUP, SUBMISSION WX12

Origins of the principles

- 2.1.3 The information privacy principles, established in accordance with the OECD’s 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (the “OECD Guidelines”), concern:
- the collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
 - access by each individual to information relating to that individual and held by public and private sector agencies.
- 2.1.4 The OECD Guidelines contain their own set of 8 principles, known respectively, as the:
- collection limitation principle;
 - data quality principle;
 - purpose specification principle;
 - individual participation principle;
 - security safeguards principle;
 - openness principle;
 - use limitation principle;
 - accountability principle.
- 2.1.5 The information privacy principles do not directly repeat the OECD principles but are designed to suit New Zealand law and circumstances and to be somewhat more precise. They owe much to the principles in the Australian Privacy Act 1988 although there are notable differences.

Principles or sections?

- 2.1.6 Many modern privacy laws contain sets of information privacy principles, data protection principles or fair information principles. For example, amongst common law countries there are sets of principles in the laws in the UK, Ireland, Australia and Hong Kong. Principles have been proposed for laws under consideration in Victoria and New South Wales. However, not all data protection or privacy laws set out principles. The Canadians legislated to implement the OECD guidelines in a more traditional manner with the content of what are principles in our Act set out as sections in a statute.
- 2.1.7 In New Zealand, the former Information Authority devised its own set of principles concerning collection, use (including disclosure) and access (including correction).¹ Notwithstanding the usefulness of principles conceptually, and its support for privacy legislation to be based on a generally applicable set of principles, the Authority was not convinced of the merit of including the principles themselves directly in legislation. Its 1988 report stated:

“Should there be principles or rules?

It was suggested that consideration should be given to having ‘principles’ instead of ‘rules’ in the legislation that governs collection and use of personal information. The United Kingdom Data Protection Act and the proposed Australian Privacy Bill are cited as examples of this approach. However, the Canadian, USA, Quebec and Ontario legislation can be quoted as examples of a rules approach. The latter Acts are clearer for all who operate the legislation to understand - those collecting, using and supplying the information and for the complaints review body.”²

- 2.1.8 Notwithstanding the Information Authority report, the two bills brought before the New Zealand Parliament substantially dealing with the subject each set out a series of principles.³ A decisive factor may have been the enactment of the Australian Privacy Act 1988 with a set of principles. New Zealand, of course, has a

¹ Information Authority, *Personal Information and the Official Information Act: Recommendations for Reform*, 1987, page 12.

² Information Authority, *Report on the Subject of Collection and Use of Personal Information*, May 1988, AJHR E27B, paragraph 25.

closer economic relationship with Australia than the North American jurisdictions which have adopted a “rules” approach. By the time the New Zealand bill was introduced the Australian Act was successfully operating for several years.

- 2.1.9 Now that the Privacy Act has operated for five years with a set of principles it would be an unattractive proposition to rewrite the law in substantially the same fashion with a “rules” approach. Nonetheless, it is acknowledged that the use of “principles” in legislation is unusual and the novelty of the legislative approach can give rise to interpretational issues over and above the content of the principles.⁴ There has been some generalised criticism that the principles make the law too imprecise and that something more prescriptive is necessary so that lawyers can explain how the law applies to specific fact situations. My experience is that those who are working on a day to day basis with the Act do not make this complaint. They see the flexibility in the principles. Lawyers look for precedent decisions and there have been few of these. That is probably the real source of the criticism of the principles by those not familiar with how the law is working in practice.
- 2.1.10 In a sense the Information Authority’s distinction between “principles” and “rules” is not entirely valid - principles can be “rules” as effectively as other sections in a statute. Fashioning parts of the statute into principles is not necessarily more significant than, say, placing material in a schedule.⁵
- 2.1.11 I do not recommend a departure from the Act’s approach in establishing a set of principles. My primary examination in respect of the principles has been directed towards their content and coverage - is any change necessary or desirable? I also took the opportunity of consultation to canvass whether there should be any new principles.⁶

SECTION BY SECTION DISCUSSION

2.2 SECTION 6 - Information privacy principles

- 2.2.1 Section 6 sets out the 12 information privacy principles. The principles are based upon the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and, in many respects, have been copied from the principles in the Australian Privacy Act 1988 (with some important changes). Throughout the principle by principle discussion which follows reference is made to both the OECD Guidelines and the Australian principles.
- 2.2.2 Also included in the discussion is reference to similar principles, and provisions, in comparable legislation in other jurisdictions and, in some cases, in international instruments. For the most part the thinking behind the principles can be dated to 1993 (when the select committee concluded its examination), 1991 (when the Privacy of Information Bill was finalised and introduced) or 1988 when the Australian principles were enacted.⁷ Accordingly, it has been

³ See the Hon Peter Dunne’s Information Privacy Bill and the Privacy of Information Bill. There were two much earlier bills, the 22 clause Preservation of Privacy Bill 1972 and the 18 clause Privacy Commissioner Bill 1974, but neither addressed information privacy issues in a substantive way. The 1972 bill would have required registration of computer installations with individual access rights while the 1974 bill would have done little more than establish a Commissioner.

⁴ Discussed in my address to the 1996 NZ Law Conference “Principles in Practice: Challenges for Lawyers”.

⁵ Having said that, the Act makes some distinctions between material in the principles and otherwise but this is a matter of statutory detail rather than the fact that they are labelled “principles”.

⁶ Forty-seven submissions were received on the discussion paper on the existing privacy principles with a further 27 on possible new privacy protections.

⁷ Indeed, one might even delve further and attribute some of the thinking to 1980, the date of the OECD Guidelines, which were themselves a culmination of 1970s experiences.

valuable to test the principles, and their drafting, against approaches taken in recent privacy legislation. There has been a considerable amount of recent legislation to ponder as can be seen at Appendix C.

2.2.3 In looking at other statutes, I have concentrated my attention on comparable jurisdictions. I have found material of value in the Canadian provincial legislation - particularly the British Columbia Act (upon which many of the subsequent provincial laws have been modelled). I have also had regard to the Hong Kong law since, like the New Zealand Act, it covers both the public and private sectors. I am aware that the New Zealand Act was studied by those responsible for drafting the Hong Kong law.

2.2.4 In addition to the influence of the OECD Guidelines and the Australian Act on the shape of the principles, there are several specifically New Zealand influences which I have kept in mind and have occasionally referred to in the report. Principal amongst these was the work of the Justice and Law Reform Select Committee which studied the Privacy of Information Bill. A further major influence in respect of principles 6 and 7 is the official information legislation which had as its origin the reports of the Danks Committee.

2.3 PRINCIPLE 1 - Purpose of collection of personal information

International origins and comparisons

2.3.1 Principle 1 is derived in part from the OECD collection limitation principle which provides:

“Collection limitation principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means, and where appropriate, with the knowledge or consent of the data subjects.”

2.3.2 The OECD collection limitation principle is supplemented by a “purpose specification principle” and “use limitation principle” which ensure that the purposes for which information are collected are made plain and any subsequent use and disclosure is limited to such purposes. The Act, in common with the Australian Privacy Act, sets out the collection, purpose specification and use and disclosure controls in separate principles. The Council of Europe Convention No. 108 is of similar effect but combines obtaining personal data and constraint on subsequent use into a single provision often referred to as the “finality principle” (although that term is not actually used in the text of the Convention).⁸ The most recent European restatement of the concept is contained in the European Union Directive on Data Protection which states:

“Member states shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.”⁹

2.3.3 The new UK Data Protection Bill’s equivalent to principle 1 has been prepared to meet the requirements of the EU Directive. It states:

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.”¹⁰

⁸ Convention No 108, article 5.

⁹ EU Directive on Data Protection, article 6(1)(b).

¹⁰ Data Protection Bill [HL], (UK), 4 June 1998 version, Schedule 1, Part I, Principle 2.

“Principle 1 has been of great educational benefit, forcing us to consider the necessity and worth of all information we collect, not just personal information.”

- FRANKLIN DISTRICT COUNCIL, SUBMISSION K8

2.3.4 The Hong Kong privacy law, which was passed after the Act, closely follows the New Zealand and Australian models but adds an additional paragraph (c). It states in full:

- “Personal data shall not be collected unless:
- (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
 - (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
 - (c) the data are adequate but not excessive in relation to that purpose.”¹¹

2.3.5 The Hong Kong ordinance was largely based upon recommendations of the Law Reform Commission of Hong Kong but the additional paragraph (c) does not appear to have originated from the Commission’s report.¹² The Law Reform Commission explicitly recommended adoption of the OECD collection limitation principle. It appears that the reference to “adequate but not excessive” is an attempt to combine the language of the European instruments with that of the OECD collection principle.¹³ This may have been done to more clearly ensure “adequacy” in terms of the EU Directive which was an explicit consideration for the Hong Kong Government.¹⁴

2.3.6 The notion of collecting “adequate but not excessive” information is consistent with the OECD Guidelines even though the phrase is not used. In my view, something very similar is required by the word “necessary” in our own principle 1. If the collection of the information is “excessive in relation to the purpose” it may equally be argued that the information is not “necessary for that purpose”. Although the Hong Kong principle appears to have achieved a good synthesis between the OECD guidelines and the EU Directive on this issue I do not recommend the adoption of its paragraph (c) in our principle. While the Hong Kong approach may, on balance, be preferable to our own principle 1 I do not think that the difference would warrant change from a principle with which users of the Act have become familiar. Further, I do not believe that the absence of the words “adequate and not excessive” would concern the Europeans when judging the adequacy of the safeguards provided by our law.

2.3.7 Most submissions expressed satisfaction with principle 1.¹⁵

2.4 PRINCIPLE 2 - Source of personal information

2.4.1 Principle 2 provides that where an agency collects personal information, the agency must collect the information directly from the individual concerned. There are a variety of exceptions set out in principle 2(2).

Rationale, origins and overseas comparisons

2.4.2 The rationale for principle 2 might be explained in several ways:

- by directing agencies to collect information directly from the individual, the individual concerned is empowered to refuse participation in the infor-

¹¹ Personal Data (Privacy) Ordinance 1995 (Hong Kong), Schedule 1, principle 1(1).

¹² See Law Reform Commission of Hong Kong, *Report on the Reform of the Law relating to the Protection of Personal Data*, 1994, paragraphs 9.5 and 9.15.

¹³ The phrase “adequate, relevant and not excessive in relation to the purposes for which they are collected” is a phrase which appears in article 6(1)(c) of the EU Directive on Data Protection.

¹⁴ EU countries must place restrictions on the transfer of personal data to countries which do not provide “adequate” safeguards - see EU Directive on Data Protection, article 25 discussed at paragraph 2.18.12.

¹⁵ See submissions K8, K9, K11, K14, K18, K20-K22, K25, K27, K28 and S13. Submissions K10, K12, K13, K19 and S19 thought it could be improved.

“Telecom believes that, generally speaking, principle 1 has worked satisfactorily in operation. It is sufficiently broad to allow the flexibility that is required in connection with normal business operations.”

- TELECOM NEW ZEALAND LTD,
SUBMISSION K12

“In many investigations Inland Revenue do source information from third parties. While in the majority of these instances the taxpayer is aware that this is taking place in others it is standard investigation technique to obtain information covertly. In many instances it is not appropriate to provide the third party with an explanation of purpose. To do so would not only reduce the effectiveness of the investigation it may well be a breach of the individual’s privacy.”

- INLAND REVENUE
DEPARTMENT, SUBMISSION K20

- information collection or to provide information on conditions;
- by constraining the circumstances in which an agency can collect information from a source other than the individual concerned, collection processes are channelled back to requests directly of the individual to which the principle 3 safeguards apply;
- collection from a source other than the individual, when the individual is in a position to provide the information directly, constitutes an affront to the individual’s autonomy - characterised by the phrase “talking about me behind my back”;
- it is an attempt to give effect to the OECD collection limitation principle which provides that personal data should be obtained, where appropriate, with the knowledge of the data subject;
- information collected might be more accurate if obtained directly from the individual concerned.

2.4.3 Nonetheless, there are circumstances where it would be unreasonable or make no sense to insist on collection of information directly from the individual concerned. For this reason, the relatively broad exceptions often apply to collections of information. Therefore, the scope of the exceptions is of as much importance as the way that the basic principle itself is framed.

2.4.4 Principle 2 does not always have a direct equivalent in information privacy laws overseas. One of its origins may have been the Information Authority’s recommendation for a collection provision which would have provided:

“A Department or Minister of the Crown or Organisation shall collect the personal information directly from the person to whom it relates except:

- (a) where the information is already publicly available; or
- (b) where the person authorises another method of collection; or
- (c) where such collection would prejudice the purpose of collection; or
- (d) where it would be of benefit to the person.”¹⁶

The Information Authority explained that “wherever possible in the interests of fairness and accuracy, information should be collected from the subject, particularly when the information may be used in decisions affecting that person.”¹⁷

2.4.5 While the Australian Privacy Act has no direct equivalent to principle 2, something similar has been proposed in the Australian National Principles for the Fair Handling of Personal Information which provides:

“Where it is reasonable and practicable to do so, an organisation should collect personal information directly from the subject of the information.”¹⁸

Exceptions

2.4.6 The exceptions to principle 2 are similar in most material respects to the sets of exceptions in principles 3, 10 and 11. The exceptions are broader than were proposed when the principle was introduced in the Privacy of Information Bill. In particular, the select committee added exceptions relating to:

¹⁶ Information Authority, *Personal Information and the Official Information Act: Recommendations for Reform 1987*, page 27.

¹⁷ *Ibid*, page 28.

¹⁸ Australian Privacy Commissioner, *National Principles for the Fair Handling of Personal Information*, February 1998, principle 1.4.

- law enforcement interests - paragraph (d)(i);
- the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue - paragraph (d)(ii) and (iii);
- the conduct of court or tribunal proceedings - paragraph (d)(iv);
- circumstances where the information will be used in a form in which individuals are not identified - paragraph (g)(i);
- information to be used for statistical or research purposes - paragraph (g)(ii); and
- exemptions obtained under section 54 - paragraph (h).

2.4.7 Although the exceptions are relatively broad - broader for instance than proposed by the Information Authority or in the Australian Privacy Commissioner's new national privacy principles - they appear to have worked satisfactorily in operation. I have no present recommendations for reform.

Notice to individual when collecting from another source

2.4.8 Where an exception applies an agency is permitted to collect information from a source other than the individual concerned. In such circumstances, the individual will not be entitled to the explanations required under principle 3 since those apply only in relation to collection directly from the individual concerned. Given the breadth of the exceptions, there may be a considerable amount of information collection activity carried out without the individual ever being made aware.

2.4.9 In some cases, this matters very little. For example, pursuant to the "publicly available information" exception a collection might be made by an agency from a "publicly available publication", such as a telephone directory. People are aware that the directory is used in such a fashion and would generally have little or no concern. However, in other circumstances, particularly where the information will be used in a way that affects their interests, the individuals affected may be very much concerned about enquiries being made and information collected without their knowledge. In only a small minority of cases, usually involving investigation which will be affected by the individual being made aware of the collection of information, is it necessary to withhold from the individual the fact that the enquiries are being made.

2.4.10 The principles could tackle the problem in one of several ways. The way that I have addressed the issue in the Health Information Privacy Code is by reducing the number of exceptions to principle 2 and by modifying principle 3 so that explanations are also given where the source of the information is the representative of the individual (a common category of health sector collections from a source other than the individual concerned). An alternative approach, taken in the Australian Privacy Commissioner's national privacy principles, is to provide that if an agency collects information from someone else that it should, where possible, make the individual concerned aware that it has done so.¹⁹

2.4.11 The new Australian principle suggests a promising approach to this problem. However, although the new Australian principles have been developed after extensive consultation with a wide range of businesses, consumers, non-profit organisations and governments, they have not as yet been implemented in an enforceable manner by law or otherwise. It is also intended that they be reviewed later this year or early next year. Therefore, it may be prudent to postpone any consideration of adopting a principle such as that until it has been further refined and implemented in Australia.

¹⁹ *Ibid*, principle 1.5. This states that "where an organisation collects personal information from a third party, it should take reasonable steps to ensure that the subject of the information is or has been made aware of the matters listed under item 1.3 above."

"There are conceivably occasions where a person's privacy could be infringed if an agency were told why the information was being collected. On the other hand there are instances when a parent is being asked for information about a child has a legitimate interest in being told what the information will be used for. The parent is providing information on behalf of an individual who is not fully able to act on its own behalf. Only in such circumstances should an agency give an explanation as to the purpose of collection."

- STATE SERVICES COMMISSION,
SUBMISSION S11

2.4.12 In consultation I sought views on whether principles 2 or 3 should be modified to oblige agencies to explain the purpose for which information is required when collecting personal information from someone other than the individual concerned. The question attracted 24 submissions. Fourteen were in support of the proposed change²⁰ with 9 opposed.²¹ Submissions both in favour and opposed to the proposition mentioned that explanations as to the purpose for collecting information from a third party would be appropriate in some circumstances but not others.²² A common refrain was that telling a third party the purpose of collection might diminish the individual's privacy in some circumstances. One submission suggested that the agency collecting the information should not be obliged to explain the purpose but the recipient of the request, if it actually released the information, should tell the individual that it had done so (submission K21). Others suggested that it would be appropriate for an explanation as to the purpose of the request to be provided where the collection was from a representative of the individual, that is a person who stands in the place of the individual with a responsibility to protect the individual's interests.²³

2.4.13 The discussion paper offered an alternative that principle 2 or 3 be amended to require an agency to tell the individual concerned if the agency intended to collect information from a third party. Again, responses were relatively evenly split. Fourteen submissions said that this should be required²⁴ while 11 submissions opposed such a requirement.²⁵ It is plain that a suitable rule, appropriate to all circumstances, might be difficult to achieve. The matter should be revisited at a future date when experience under the proposed Australian principle can be evaluated.

2.5 PRINCIPLE 3 - Collection of information from subject

2.5.1 Principle 3 is one of the most important provisions in the Privacy Act. It brings together features of several of the OECD principles. Underlying the principle are ideas of openness: that collection of personal information should be done with the knowledge or consent of the individual concerned, that the purposes for which information is collected should be specified no later than the time of collection and subsequent use limited to fulfilment of those and compatible purposes, and there should generally be transparency about information collection policy and individual participation in that process.

2.5.2 The principle requires that where an agency collects personal information directly from the individual concerned, the agency take reasonable steps to ensure that the individual is aware of certain matters. Those steps are to be taken before the information is collected or, if that is not practicable, as soon as practicable thereafter. There are some exceptions where the individual does not have to be made aware of the various matters.

Explanations required by principle 3(1)

2.5.3 The principle requires individuals to be made aware of a number of items:

- the fact of collection;
- the purpose for which the information is being collected;
- the intended recipients;
- the name and address of the agency collecting and that will hold the information;

²⁰ Submissions K3, K8, K11 - K13, K18, K19, K25, K28, S21, S24, S36 and S42.

²¹ Submissions K9, K14, K20, K21, S6, S13, S15, S25 and S56.

²² See, for example, submissions K12, K18, K19, K20, K28, S6, S11, S15 and S25.

²³ See, for example, submissions K28, S6, S11 and S15.

²⁴ Submissions K3, K10, K11, K12, K18, K19, K25, K29, S6, S19, S21, S24, S36 and S42.

²⁵ Submissions K8, K9, K13, K14, K20, K21, K28, S13, S15, S25 and S45.

“The obligation to explain to a third party the purpose of collection may result in the inadvertent disclosure of personal information (eg locating a debtor). There should be an obligation to tell an individual that information has been collected about him or her as soon as practicable and not inconsistent with the purpose of collection.”

- KATHRYN DALZIEL,
SUBMISSION S6

- any law authorising or requiring the collection and whether that law makes the supply of the information voluntary or mandatory;
- the consequences if the request for information is not provided; and
- the rights of access and correction.

2.5.4 The required explanations in principle 3(1) remain the same as those introduced in the Privacy of Information Bill. I have compared the principle to similar requirements appearing in other privacy laws and it is broadly similar to most and, from an individual’s perspective, better than many in terms of the breadth of useful information required to be conveyed. For example the absence in the Australian Privacy Act of an equivalent to our principle 3(1)(f) has been described as a “significant gap” in the Australian privacy principles.²⁶

2.5.5 A few laws require other details to be provided. For example, the British Columbia law requires that the individual concerned be made aware of:

“The title, business address and business telephone number of an officer or employee of the public body who can answer the individual’s questions about the collection.”²⁷

While that requirement is pitched at a level that is useful for an individual I do not propose it for our own principle 3. The British Columbia Act primarily applies to the provincial and local government sectors. With that limited application a precise requirement of the type described is probably appropriate and useful. With a far larger range of public and private bodies covered by our Act I prefer to keep the principle at the present level of generality requiring simply the name and address of the relevant agency.²⁸

2.5.6 Some overseas principles indicate that the individual should be made aware of certain information handling policies or practices of the agency. For example, the “notice principle” in the National Information Infrastructure Principles (USA) states:

“Information users who collect personal information directly from the individual should provide adequate, relevant information about what steps will be taken to protect its confidentiality, integrity and quality.”²⁹

2.5.7 The NII principles have not been implemented in the USA in an enforceable fashion and therefore do not offer a useful precedent to draw on. By contrast, the Hong Kong law has a principle, not linked to collection of information from the individual concerned, which requires certain information on agencies’ practices to be made available. It states:

“PRINCIPLE 5 - Information to be generally available
All practicable steps shall be taken to ensure that a person can:
(a) ascertain a data user’s policies and practices in relation to personal data;

²⁶ Australian Privacy Commissioner, Privacy Protection in the Private Sector: Response to Discussion Paper issued by the Attorney-General, December 1996, page 6.

²⁷ Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 27(2).

²⁸ Nonetheless, a provision which might be worth considering at a later date, if successfully implemented in Australia, is the simple formulation in the Australian National Principles for the Fair Handling of Personal Information which refers to “the identity of the organisation and how to contact it” (principle 1.3(a)).

²⁹ Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, “Privacy and the National Information Infrastructure: Principles for providing and using personal information”, final version 6 June 1995, principle IIB.

“The items currently listed in (a) to (g) reflect an appropriate balance between ensuring that individuals are protected and not imposing undue burdens on agencies. The items currently required in principle 3 explanations are sufficient to allow individuals to exercise their rights in relation to their personal information.”

- MINISTRY OF JUSTICE,
SUBMISSION K28

- (b) be informed of the kind of personal data held by a data user;
- (c) be informed of the main purposes for which personal data used by a data user are or are to be used.”³⁰

2.5.8 There was some support in submissions for a principle, not linked to collection, to require openness regarding agency information practices.³¹ I suggest that such matters might better be dealt with in the framework of our law within specifically issued codes of practice rather than a new principle. That would allow for any obligations to be particularised to a sector or type of information or activity. As this would not necessarily be able to be achieved easily by simply modifying an existing principle I suggest that the power for issuing codes of practice should be broadened to expressly refer to the matter detailed in principle 5(a) of the Hong Kong law.



RECOMMENDATION 18

Section 46(4) should be amended to provide that a code of practice may require an agency to take all practicable steps to ensure that an individual may ascertain the agency’s policies and practices in relation to particular personal information.

2.5.9 Most submissions were opposed to adding any further explanations to principle 3(1)³² or indeed to making any changes to items (a) to (g) of principle 3(1).³³ However, a few submissions favoured change including that:

- consideration be given to simplifying or clarifying the explanations;³⁴
- item (b), which simply refers to “the purpose”, ought to be reconciled with principle 3(4)(d) which refers to “the purposes”.³⁵

Purpose or purposes

2.5.10 Principle 1 speaks of the collection of personal information for a “purpose”. It has been suggested during consultation, and earlier when the Privacy of Information Bill was before the select committee, that it is confusing to refer solely to single “purpose” when there might be more than one purpose of relevance. The singular is also used in principles 1(a) and 8. Some of the other principles, and the exceptions to the principles, use “purposes”.

2.5.11 The proposition to replace the reference to “purpose” by “purpose or purposes” was rejected by the select committee because on normal statutory interpretation the term would be read that way in any case. In particular, section 4 of the Acts Interpretation Act 1924 states:

“Words importing the singular number include the plural number, and words importing the plural number include the singular number.”

2.5.12 I think that the position will be plainer for users of the statute if the phrase “purpose or purposes” is substituted. My concern extends to lay people who are not familiar with normal rules of statutory interpretation.

³⁰ Personal Data (Privacy) Ordinance 1995 (Hong Kong), Schedule 1.

³¹ Submissions R4, R5, R6, R8, R12, S24, S42 and S56 were in favour. Submissions R3, R13, S3 and R14 were opposed.

³² Twelve of the 15 submissions opposed adding further items (K8, K9, K12, K14, K18, K19, K21, K25, K27, K28, S11 and S13). Submissions K11 and S42 liked the British Columbia requirement to give a telephone number with K13 favouring greater advertisement to individuals of the ways to contact a privacy officer.

³³ Thirteen of the 18 submissions on this point saw no case for change (see submissions K8, K9, K11, K12, K14, K18, K20, K25, K27, K28, S6, S11 and S13).

³⁴ Submissions K6 and S42.

³⁵ Submission S19.

“Overall the items listed are useful and give the information giver certain rights of control and protection.”

- NEW ZEALAND COLLEGE OF MIDWIVES, SUBMISSION K13

“We consider that principle 3(1) is too unwieldy as it is without needing to expand on the amount of information than an agency should provide.”

- BAYNET CRA LTD, SUBMISSION K21

**RECOMMENDATION 19**

Information privacy principles 1, 3(1) and 8 should be amended to substitute the phrase “purpose or purposes” for the word “purpose”.

Principle 3(2) and (3)

2.5.13 Principle 3(2) makes it clear that the steps required to be taken in principle 3(1) must be taken before the information is collected but that if that is not practicable the steps are to be taken as soon as practicable thereafter. This provision is copied from principle 2 of the Australian Privacy Act.

2.5.14 Principle 3(3) provides that an agency is not required to take the steps referred to in principle 3(1) if the agency has taken those steps in relation to the collection from that individual of the same or similar information on a recent previous occasion. This subclause is not taken from the Australian Privacy Act and did not appear in the Privacy of Information Bill as introduced. It was added by the select committee to reduce, in a modest way, potential compliance costs for agencies. It also ensures that unneeded and unwanted explanations are not unnecessarily repeated.

Exceptions

2.5.15 Principle 3(4) contains exceptions which are almost identical to exceptions found in principle 2, 10 and 11. The list is far more extensive than was originally contained in the Privacy of Information Bill, which solely contained an exception similar to the present exception (d). The equivalent principle in the Australian Privacy Act contains no exceptions at all, with resultant emphasis being placed upon the “reasonableness” or “practicability” of giving explanations in difficult circumstances.

2.5.16 Approximately two thirds of the 19 submissions received in relation to principle 3(4) expressed comfort with the present exemptions. The remainder were concerned about the exceptions contained in principle 3(4)(a) and 3(4)(f)(ii) relating to individual authorisation, and statistical and research purposes, respectively.

Authorisation for non-compliance

2.5.17 Principle 3(4)(a) permits an agency to dispense with explanations anticipated by principle 3(1) when “non compliance is authorised by the individual concerned”. This exception could be problematic if authorisations are sought on standard forms where there is imbalance in bargaining position between individual and agencies. The exceptions might even be characterised as an authorisation to “contract out” of one of the key provisions in the Act.

2.5.18 In order for an authorisation to be meaningful in terms of the Act’s principles it should be an *informed* authorisation which would be unlikely to be the case if the individual is denied the explanations anticipated by principle 3(1). It also upsets the scheme of the principles, such as those governing use and disclosure, if the purpose of collection is not specified at the outset. The complementary nature of the principles is upset by this exception.

2.5.19 I have concluded that principle 3(4)(a) should be repealed. It is an unusual provision not generally found in the equivalent exceptions in overseas privacy laws. I can find no justification for it within the OECD guidelines on which the Act is based.

**RECOMMENDATION 20**

Information privacy principle 3(4)(a) should be repealed.

Statistical or research purposes exception

2.5.20 Concern has also been expressed in relation to the exception contained in principle 3(4)(f)(ii) whereby agencies need not make individuals aware of the matters in principle 3(1) where the information:

“It is difficult to justify an individual authorising a waiver of the explanation required to enable them to make informed decisions about their personal information. In order for an authorisation to be meaningful in terms of the Act’s aims and principles, it should be an *informed* authorisation.”

- MINISTRY OF JUSTICE, SUBMISSION

K28

“Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.”

2.5.21 I recognise an important public interest in statistical and research purposes. The exceptions which exist in principles 2, 10 and 11 are, to my mind, appropriate and essential features of the scheme of the Act. However, I am not convinced that the gathering of statistics, or the fact that the objective is research, justifies an exception to principle 3(1) where the collection of *personal information is directly from the individual concerned*. I emphasise that principle 3:

- concerns only the collection of “personal information”; and
- applies where the collection of the information is “directly from the individual concerned”.

An exception is not needed where:

- collection is from individuals whose identities are not known (such as anonymous street interviews where identifying details are not taken); or
- collection is from sources other than the individual concerned (such as research concerning existing records).

2.5.22 Collection of information directly from the individual for the purposes of research or statistics will typically involve an interview or a request for the individual to complete a form. I cannot see that there is anything inherent in the nature of research, or the collection of statistics, which should relieve an agency collecting personal information from explaining, amongst other things:

- the purpose of the collection;
- the intended recipients;
- the identity of the agency that is asking the questions;
- whether the supply of the information required under law is voluntary or mandatory.³⁶

2.5.23 Nor, do I believe that any significant difficulty should be caused to legitimate and ethically conducted research or statistics gathering in providing such explanations. I should add that in particular circumstances there may be a reason to rely upon one of the other exceptions to delay the giving of certain explanations until the collection is complete. For example, responses to a survey which are supposed to be unprompted might be affected if the name of the agency which has commissioned the research, and which is to be the recipient of the information, is given out in advance of the questions being posed.³⁷ In such cases, I expect that principle 3(2) and 3(4)(d) may be relied upon so that the requisite explanation is given after the interview or form is completed.

2.5.24 I received a helpful submission from the Association of Market Research Organisations (AMRO) which explained its position and the importance attached to the relevant exemptions to the information privacy principles. While it opposed the removal of the exemptions I believe that its concerns will be largely met so long as the relevant exemptions to principles 2, 10 and 11 are retained. In fact, it appears that the requirements of AMRO’s Code of Practice require members to comply with obligations which are remarkably similar to principle 3 in various respects. For example, the code³⁸ provides as follows:

“Respondents’ cooperation in a market research project is

³⁶ There would be few statistical or research collection of personal information which are conducted under law and which are mandatory. The prime example would be those undertaken by Statistics New Zealand and I have little doubt that the practice of that agency would be to tell recipients of the sort of matters specified in principle 3(1).

³⁷ I expect that in many cases no actual personal information will be transferred to the commissioning organisation but instead just the statistical research results.

³⁸ Code of Practice of the Market Research Society of NZ Inc, January 1995. This is an industry code of conduct, not a code issued under the Privacy Act.

“It is not appropriate for any person to be expected to disclose personal health information without knowing its use. While there is definite benefit in the gathering of statistical or research data it must never be done without disclosure of its use to the individual who volunteers that information.”

- NZ COLLEGE OF

MIDWIVES, SUBMISSION K1.3

entirely voluntary at all stages. They must not be misled when being asked for the cooperation.” (Article 3)

“If the respondent is supplying information not in a private capacity but as an officer of an organisation or firm it may be desirable to list the respondent’s organisation in the report. The report, shall not, however, enable any particular piece of information to be related to any particular organisation or person, except with prior explicit permission from the relevant respondent, who shall be told of the extent to which it will be communicated. This requirement does not apply in the case of secondary analysis of published data.” (Article 5)

“The researcher must avoid unnecessary intrusions on respondents’ privacy”. (Article 6)

“Respondents’ anonymity must always be strictly preserved unless they have explicitly agreed to the contrary. The researcher must ensure that the information they provide cannot be linked to specific individuals or organisations without such permission. It is the researcher’s responsibility to inform clients of respondents’ anonymity rights”. (Article 7)

“In any case where respondents are asked for permission to disclose their name and/or address to anyone outside the research agency:

- (a) the respondent must first be told to whom the information would be supplied and the purposes for which it will be used, and also;
- (b) the researcher must ensure that:
 - (i) the information will not be used for any non-research activity;
 - (ii) the information will not be published in a form that could reasonably be expected to identify the respondents; and
 - (iii) the recipient of the information has agreed to conform the requirements of this code.” (Article 8)

“Respondents must be told at the time of the interview when observational recording techniques are to be used, except when these are used in a public place. If a respondent so wishes, the record or relevant section of it must be destroyed or deleted. Respondents’ anonymity must not be infringed by use of such methods”. (Article 10)

“Respondents must be able to check without difficulty the identity and bona fides of the researcher and to obtain an answer to any reasonable query about the purposes and content of the research. Each interviewer must be able to be identified in a way that specifies his or her name and organisation. The name and address/telephone number of the research company must be made available to the respondent at the time of the interview.” (Article 11)

2.5.25 A further difficulty with the exception is that it does not make clear what it is to “publish” the information. Clearly the constraint on publishing information in a way that identifies the individual is an important protection. However, it

may well be that the disclosure of the information from the agency which collects it, as part of a research or statistical project, to another agency, such as an agency which has commissioned the research, may not be characterised as “publication”. If that view were to be taken it would mean that the individual is completely left without protection in a privacy sense and is in the dark as to why information was collected and who will get hold of it. If the exception were to be retained it ought to be narrowed so that it may only be relied upon if the information from which individuals may be identified is to remain solely with the agency that collects the information. However, in my view the exception should be repealed totally rather than simply refashioned in that way.



RECOMMENDATION 21

Information privacy principle 3(4)(f)(ii) should be repealed.

2.6 PRINCIPLE 4 - Manner of collection of personal information

2.6.1 Principle 4 is relatively brief and straightforward and prohibits the collection of personal information by an agency by unlawful means or unfair or unreasonably intrusive means. The principle seeks to give effect to the OECD collection limitation principle and its constituent parts are drawn from information privacy principles 1(2) and 3(d) in the Australian Privacy Act.

2.6.2 The principle has featured in a number of complaints to my Office. Those reported in case notes to date have included:

- a private investigator, in breach of the Private Investigators and Security Guards Act 1975, photographing another person without that person’s prior written consent (case note 3734);
- hidden video camera surveillance in a workplace locker-room (case note 632);
- a private investigator posing as a potential guest in accommodation premises (case note 6314);
- a police officer telephoning a school to seek children’s address on the pretext of returning stolen property whereas in fact in context of deportation of father (case note 11536);
- a private investigator using a ruse of being a potential buyer to enter a home and videotape the occupants (case note 14824).

2.6.3 I have no suggestions for amendment of principle 4 which was considered by most submissions to have worked well.³⁹

2.6.4 The Complaints Review Tribunal has not yet had the opportunity to consider principle 4 although interestingly the courts, in their criminal jurisdiction, have. The case of *R v Wong-Tung*⁴⁰ concerned the lawfulness of attaching a telephone analyser to a telecommunications network. A telephone analyser is a device which enables the recording of data generated as a result of telecommunications made using a telephone line. The data recorded is restricted to information about the telecommunication (such as the number called, the time called, and the duration of the call) and does not include the content of the telecommunications.

2.6.5 The practice of attaching telephone analysers in the course of criminal investigations had grown up since the 1980s without any regulation, in contrast to the strong controls on the interception of the content of private communications. From 1993 the Privacy Act essentially regulated aspects of the practice which was not entirely satisfactory from the perspective of telecommunication companies, law enforcement agencies or the privacy interests of individuals.

³⁹ See submissions K8, K9, K12, K13, K14, K18, K19, K21, K25, K27 and K28.

⁴⁰ (1996) 2 HRNZ 272. It is unnecessary to examine the facts and findings of that case here.



“One of the key positives of principle 4 is the general nature in which it is prescribed. It is not burdened with large numbers of exceptions and restrictions. It should be maintained in the current format.”

- INLAND REVENUE

DEPARTMENT, SUBMISSION K20

Accordingly, I welcomed the recent enactment of provisions prohibiting the attachment of telephone analysers except with a judicial “call data warrant”.⁴¹ I consider that something similar ought to be considered for covert video surveillance for law enforcement purposes as it is unlikely that principle 4 or the other principles will be sufficient to appropriately constrain or control the activity which leads to similar strong privacy concerns.



RECOMMENDATION 22

Consideration should be given to establishing a judicial warrant process in relation to the use of covert video surveillance in the investigation of offences.

2.7 PRINCIPLE 5 - Storage and security of personal information

2.7.1 Principle 5 is derived from the OECD security safeguards principle which provides:

“Security safeguards principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.”⁴²

2.7.2 Principle 5 is closely modelled on principle 4 of the Australian Privacy Act. In addition to paragraph (a), which closely follows the approach of the OECD security safeguards principle, there is, in both the New Zealand and Australian Acts, a second paragraph placing security obligations on agencies where information is given to a person in connection with the provision of a service to the agency.

2.7.3 Principle 5 is clearly expressed and easily understood by agencies. It does not appear to have caused significant interpretational problems in operation.

Recent international security safeguards developments

2.7.4 Since the 1980 OECD guidelines were released there has been a significant amount of work undertaken internationally on refining information security principles. In 1992 the OECD released its Guidelines for the Security of Information Systems (“the 1992 Guidelines”). These built upon the security safeguards principle in the 1980 Guidelines and contained 8 further principles, being the:

- accountability principle;
- awareness principle;
- ethics principle;
- proportionality principle;
- periodic reassessment principle;
- multi-disciplinary principle;
- integration principle;
- democracy principle.

2.7.5 The 1992 Guidelines were finalised after the Privacy of Information Bill had been drafted and introduced into Parliament and after the Privacy Commissioner Act 1991 had been enacted. Accordingly, those guidelines did not feature in the drafting of the legislation.

2.7.6 The 1992 Guidelines provide a valuable elaboration of the 1980 Guidelines and offer a recommended approach to issues concerning the security of information systems. I have concluded that there is no particular need to refer to them explicitly in the Act. I already have authority to take account of the 1992 Guidelines pursuant to section 14(b) and (c). I encourage agencies, especially public bodies and industry groups, to consider them in their development of policies concerning the security of information systems.

⁴¹ See report by the Privacy Commissioner to the Minister of Justice in respect of Part X of the Harassment and Criminal Associations Bill amending the Telecommunications Act, Telephone Analysers and Call Data Warrants, 10 September 1997.

⁴² OECD Guidelines, clause 11.

- 2.7.7 Another relevant OECD development concerns cryptography. In 1996 the OECD released guidelines for cryptography policy which contained within them a set of principles.⁴³ As the guidelines are very recent it is difficult to gauge how influential they will be throughout the OECD and international community. I am unaware of any country having yet legislated on the basis of the OECD cryptography guidelines (although some countries have legislated in respect of cryptography policy). Cryptography has become central to aspects of the debate over security of personal information and if New Zealand were to adopt a more restrictive policy in this area it would be desirable to consider the privacy and Privacy Act implications. The OECD work would be valuable in that context. In particular, I highlight principles 2 and 5 of those guidelines which provide:

“2. Choice of cryptographic methods

Users should have a right to choose any cryptographic method, subject to applicable law.

“5. Protection of privacy and personal data

The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and the implementation and use of cryptographic methods.”

- 2.7.8 Although I sought views on the issues in the consultation I do not see this review as being an appropriate vehicle to take any initiatives in respect of cryptography. Principle 5 is intentionally silent as to technical means of achieving adequate security as these will vary over time. It is unlikely that reference to a specific technique or technology, such as cryptography, would be appropriate in this principle. Nonetheless, there is a strongly held view amongst many people interested in privacy that individual access to cryptography technology is likely to be an essential means to protect privacy as we move into the Twenty-first Century and the global information society.
- 2.7.9 Other sets of privacy principles have also tackled security issues in new ways. The EU Directive on Data Protection deals with “confidentiality of the processing” and “security of processing” in articles 16 and 17 in ways which differ slightly from our own principles. The EU Directive also differs in relation to “sensitive categories of data” and the “transfer of personal data to third countries”. I deal with the latter issue in detail at paragraph 2.18.
- 2.7.10 In the USA the National Information Infrastructure principles took a novel approach to information security. They emphasised the empowerment of individuals to utilise technology to safeguard their own data. One part of the “empowerment principle” stated:

“Individuals should be able to safeguard their own privacy by having the opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions.”

- 2.7.11 The empowerment principle also stated that individuals should be able to safeguard their own privacy by having the opportunity to remain anonymous when appropriate. Anonymity is often the most effective security safeguard that individuals can adopt. Pseudonymity is also a very effective means for enhancing privacy particularly when individuals participate in transactions. Pseudonymity provides for an identifier to be assigned to an individual as a party to a transac-

“The Act should not move away from the concept of statements of principle to also prescribe the methodology by which those principles may be implemented. Legislation that has set out to define methodology has become rapidly dated as technology has changed and that the rate of technological change continues to increase. If, however, it is considered necessary to legislate on the subject of cryptology, the Bureau would take the view that the Privacy Act is not the appropriate vehicle by which to do so.”

- GOVERNMENT

COMMUNICATIONS SECURITY BUREAU,

SUBMISSION K4

⁴³ OECD, Recommendations of the Council concerning Guidelines for Cryptography Policy, 27 March 1997.

tion which is not, in the normal course of events, sufficient to associate the transaction with a particular human being. A transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party. Nonetheless, the identity of that party can be established, in appropriate circumstances by, for example, bringing together partial identifiers which have been stored separately by two or more organisations. Another approach is for an indirect identifier to be stored with the transaction and a cross index to be held which would enable the person's real identity to be divulged in specified circumstances subject to organisational, technical and possibly legal, safeguards.⁴⁴

- 2.7.12 I have no recommendations for amendment to principle 5. It has worked well and applies an appropriate standard for information security to take account of changing circumstances and the availability of new technologies. However, as the preceding discussion has suggested there is a lively international debate about information security, particularly as regards cryptography policy. The potential of privacy enhancing technologies has also focused attention on the possibilities for anonymous or pseudonymous transactions to enhance privacy. Developments in this area may not require any change to principle 5 but with the pace of change in this area being quite rapid I expect that the matter will require re-examination at the next periodic review of the Act.

Browsing or inspection of information

- 2.7.13 I have outlined elsewhere that an issue has arisen overseas, and in New Zealand, as to whether “browsing” constitutes a “use” of information under a privacy or data protection law. Browsing of information typically involves employees, who are authorised to have access to an agency's information holdings in connection with their employment on their employer's business, inspecting or browsing through files for no legitimate purpose. Sometimes employees are simply curious. Others wish to find out information about friends, family members, acquaintances or enemies. In some cases, the browsing is a precursor to the improper disclosure of the information or its sale. This can be a particular issue in relation to large databases such as those maintained by the Police, Income Support, CYPFS, and public hospitals, where it can be difficult to limit access to small numbers of staff.
- 2.7.14 Browsing is seen as an affront to privacy of the individuals concerned but it is not always easy to characterise the practice as a breach of the privacy principles. This is principally because it is debatable whether simply reading or inspecting information, but not otherwise acting upon it, constitutes a “use” of the information. Accordingly, one possible response is to define “use” in a way that encompasses the practice. I have recommended elsewhere that this be considered.⁴⁵
- 2.7.15 However, another way of tackling the issue may be to modify information privacy principle 5 so as to make it plain that agencies are required to safeguard personal information against browsing. The present obligations in information privacy principle 5 relate to loss, access, use, modification, disclosure or other misuse. The practice of browsing does not concern loss or modification of information. Generally it does involve access to information but typically the browser is a person authorised to have access to the agency's records but is doing so for purposes that have not been authorised and which are not the agency's purposes. Accordingly, the obligations relating to access are arguably not enough of themselves. Typically it is alleged that browsing does not involve use or disclosure of information - or at least any use or disclosure which can be

⁴⁴ This description of pseudonymity is taken from Dr Roger Clarke, “The Scope for Transaction Anonymity and Pseudonymity”, Fifth Conference on Computers, Freedom and Privacy, 1995.

⁴⁵ See paragraphs 1.4.103 - 1.4.111 and recommendation 16.

“New Zealand’s original principle 5 is too vague to be of much value today. Electronically stored information require safeguards that are specific to both the storage method and the system that is being used. Specific aspects of the OECD’s Guidelines for the Security of Information Systems should be included in principle 5 and not just referred to elsewhere in the Privacy Act.”

- DR LALITA RAJASINHAM, VICTORIA UNIVERSITY, SUBMISSION K1

proved. It is possible that the practice constitutes “other misuse” although that in itself may be dependent upon whether one considers browsing as “use”.

- 2.7.16 I suggest that the practice could be tackled by inserting the word “browsing” or “inspection” in principle 5(a)(ii) which will oblige agencies to take safeguards against the practice.



RECOMMENDATION 23

Information privacy principle 5(a)(ii) should be amended by inserting the word “browsing” or “inspection”.

2.8 PRINCIPLE 6 - Access to personal information

- 2.8.1 All jurisdictions which have specific privacy legislation include within that a right of access by individuals to information held about them. Principle 6 provides that right of access and it gives effect, in part, to the OECD “Individual participation principle”.

- 2.8.2 The right of access is important in a variety of ways. Lying behind privacy legislation is a recognition of an individual’s entitlement to some degree of personal autonomy. That autonomy would be illusory in many cases unless the individual can see what information is held for potential use by others. Another reason for the right of access is because of the concern that personal information to be used should be accurate and possibly the best way of ensuring such accuracy is to let the individuals see it and point out any errors. It provides some measure of accountability by agencies to the individuals whose personal information they hold and may use. Finally, an individual’s right of access tends to make other aspects of the information privacy principles self-policing. Objectionable handling of personal information might tend to come to light through the individual securing access either in the hands of the agency concerned or in the hands of another agency to which the information has been passed.

Legislative history

- 2.8.3 The Official Information Act 1982 gave everyone the right to have access to information which was held by those public sector bodies covered by the legislation. This initially was the core public service.⁴⁶ The list of bodies covered has been broadened subsequently with the main extension made in 1987 to, including others, universities, schools and public hospitals. Also in 1987 the Local Government Official Information and Meetings Act was enacted which is both a freedom of information law and a “sunshine” law (the latter feature constraining local authorities in their ability to meet in secret).
- 2.8.4 Within the overall right of access contained in the official information statutes was a special right for individuals to have access to personal information held about themselves by any of the bodies covered. There are fewer grounds for withholding such information from the individual concerned. No charge was permitted to be made for such access.
- 2.8.5 In 1993 the individual right of access to personal information was transferred to the Privacy Act and at the same time it was extended to the private sector. One significant difference between the sectors was that, in order to minimise the cost to business, private sector agencies were permitted to recover at least some of their costs from the requester. By and large, the permissible grounds under the Privacy Act upon which any agency can decline to disclose to the requesting individual what it holds about them are the same as those previously applicable under the official information statutes.

⁴⁶ Essentially, the initial application of the official information legislation corresponded to those agencies defined as a “Department”, “Minister” or “Organisation”, in section 2.

- 2.8.6 Since 1993 many thousands of New Zealanders have exercised access rights under information privacy principle 6. It is not possible to put a precise figure on the number of requests as the legislation, and the Official Information Act which preceded it, puts an emphasis upon simple procedures and the avoidance of unnecessary formalities. Accordingly, access requests need not utilise a special form or be in writing, be routed through a special officer, or be logged or counted in any particular fashion. No statistics are kept as to access requests made. However, statistics are kept in relation to complaints lodged with my office. Complaints which include access are the largest single category of complaints making up approximately 40% of the total. Further details about the number of complaints received since 1993 can be found at Appendix J. Similarly, proceedings before the Complaints Review Tribunal have predominantly concerned refusal of access requests.
- 2.8.7 There was a great deal of interest in the issues of access to personal information in the consultation process. Fifty submissions were received on the access and correction discussion paper, the most for any of the discussion papers.
- 2.8.8 The right of access to personal information is widely supported and is recognised to be an important and powerful individual right. Accordingly, in my review most of the attention in this context has been towards the detail of the access regime, notably aspects of the permitted withholding grounds and the procedural provisions for giving access, rather than the right itself. Most submissions considered principle 6 to have operated satisfactorily.⁴⁷ The issues raised and examined primarily concerned the reasons for withholding information and the procedural provisions. These are discussed in respect of Parts IV and V elsewhere in this report.
- 2.8.9 The right of access is also associated strongly with procedural fairness. Many people aggrieved at some action, or lack of action, about a matter concerning them, obtain a real satisfaction from being able to access relevant information. This accountability shines a light into what may have hitherto been dark places and can lead to a change of approach and a greater sense of responsibility by agencies.

2.9 PRINCIPLE 7 - Correction of personal information

- 2.9.1 Principle 7 provides that, where an agency holds personal information, the individual concerned has a right to request correction of the information and, if the correction is not made, to request there be a statement attached to the information that correction was sought but not made.
- 2.9.2 Principle 7 shares a similar legislative history to principle 6. The right was originally contained in the official information statutes and therefore has existed in the public sector since the 1980s. The entitlement to seek correction of personal information also gives effect to the final part of the OECD “Individual participation principle” which indicates that 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.”
- 2.9.3 A number of principle 7 complaints have been brought to me. The most common situation concerns information held on the files of credit reporting agencies which is alleged by an individual to be inaccurate, incomplete or misleading.⁴⁸ The Complaints Review Tribunal has also considered several cases involving the principle.⁴⁹

⁴⁷ See submissions K8, K9, K11-K14, K18, K21, K25 and K27.

⁴⁸ See, for example, case notes 451, 613, 909 and 1827.

⁴⁹ See, for example, *Powell v Special Education Service*, Complaints Review Tribunal, 26 July 1996, Decision No CRT 26/96, *Adams v Police*, Complaints Review Tribunal, 12 June 1997, Decision No CRT 16/97.

- 2.9.4 Most submissions on the subject considered that principle 7 had operated adequately.⁵⁰ However, two commented that:
- the principle should state that no charge may be made for an individual seeking to have information corrected (submission K11);
 - the concept of “attaching” a statement to information under principle 7(3) should be made more clearly applicable to information in electronic form (submission K12).
- 2.9.5 The first point has some validity and I address it in recommendation 65. However, with respect to the second point I consider that the Act works satisfactorily in relation to “attaching” a statement to electronic data notwithstanding that there may be a semantic issue as to whether one can truly “attach” a piece of data to another in an electronic environment. Agencies usually include the statement within the same electronic document or databank or they attach a “flag” of some sort which refers users to a hard copy record or to the location of the electronic record.
- Obligation to advise of right under principle 7(1)(b)*
- 2.9.6 Principle 7(1) confers two entitlements on individuals:
- (a) to request correction of personal information held by an agency; and
 - (b) to request that there be attached to the information a statement of the correction sought but not made.
- Principle 7(2) to 7(5) explains how the entitlement is to be acted upon by an agency. The two parts of principle 7(1) usually work adequately together because an agency which refuses to act upon a request for correction will normally volunteer to the requester, when explaining that the correction will not be made, that the requester may ask for a statement to be attached for the unchanged information. Principle 7(3) seems to make clear that the agency’s obligation to attach a statement is activated only upon a request by the individual concerned. Typically, this will be a second request by the individual unless they have earlier asked for a correction and, in lieu, for the attachment of a statement.
- 2.9.7 I suggest that the principle should be amended so that an agency is obliged to inform requesters of the entitlement to request that a statement be attached. I do not think it is necessary to go so far as to oblige agencies to actually attach such a statement in the absence of a further request from the individual although I note that this was the obligation in the corresponding provision in the Official Information Act that formerly related to correction of information.⁵¹ There was a fair measure of support for such a proposal in submissions.⁵²



RECOMMENDATION 24

Information privacy principle 7 should be suitably amended so that agencies are obliged to inform requesters, in cases where the agency is not willing to correct information, that they may request that a statement be attached to the information.

Preventing use of information for purposes of direct marketing

- 2.9.8 Direct marketing continues to be the subject of a stream of enquiries to my office. The issue is frequently couched in terms of a failure of an agency to act upon a request to delete a person’s name from a mailing list. As “correct” includes the alteration of personal information by way of deletion it is understandable that the matter is sometimes asserted to be an entitlement conferred by principle 7.

⁵⁰ See submissions K8, K9, K11, K13, K14, K18, K21, K25 and K27.

⁵¹ Official Information Act 1982, section 26(1)(b).

⁵² Twelve submissions considered that principle 7 should be more specific as to an agency’s obligation to consider and give effect to a request for correction (see submissions L2, L4, L5, L7, L13, L14, L19, S2, S7, S36, and S45).

- 2.9.9 The principle does entitle individuals to *request* deletion of details from an agency’s mailing list and to *oblige* the agency to take a decision to accept or deny the request. However, it is unlikely that an agency can be *obliged* to delete accurate information under the principle.
- 2.9.10 The principle has as its primary focus the correction of inaccurate information rather than the deletion of information which it is alleged should not be used for a particular purpose. In that sense, it might be characterised as a data quality entitlement rather than a limit upon use. One might therefore argue that principle 7 is appropriately used for removing a name from a marketing list where the individual’s details were placed on the mailing list through error but not because the details were obtained in breach of principle 3 or 11.
- 2.9.11 However, I would like to move the issue beyond the interpretation of principle 7 as it presently appears onto the issue of whether individuals should be entitled to be removed from direct marketing lists. There was support for this proposal in submissions.⁵³
- 2.9.12 An entitlement to be taken off lists used for direct marketing purposes would be easy for individuals to exercise. It would be a fairly straightforward request for agencies to respond to and to be reviewed on a complaint. At present, direct marketing complaints could involve an elaborate inquiry into the circumstances in which an individual’s details came to be placed on an agency’s marketing list. In essence this involves a check of compliance with principles 1 to 4 and possibly 10 and 11. This can be done but it will usually be more straightforward to simply take the person’s name off the list. This is how such customer complaints are frequently resolved.
- 2.9.13 Direct marketing complaints are some of the most common allegations of use of personal information obtained for one purpose for another purpose. The harm or detriment suffered by individuals is undoubtedly at the low end of the scale. However, while the harm may be minimal at an individual level, the quantity of direct marketing means that a single mail-shot may cumulatively affect and irritate many thousands of individuals and therefore be a significant breach of the collection, use and disclosure principles. In my view, the problem should be addressed with a comparatively simple mechanism which, consistent with the information privacy principles, gets to the heart of the consumer dissatisfaction. The answer is to empower individuals to demand that their details be removed from, or blocked on, lists held for direct marketing purposes. This is the approach required of members of the Direct Marketing Association by the Association’s rules. However, the DMA’s voluntary scheme has not been successful because amongst other things, it is confined to members and lacks enforcement mechanisms.
- 2.9.14 This is the approach of in the EU Directive on Data Protection which provides in article 14(b):

“The data subject’s right to object

Member states shall grant the data subject the right:

- (b) to object on request, and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used

⁵³ Eleven of 17 submissions supported the proposed right to be removed from a direct marketing list (see submissions L4, L7, L12, L14, L23, S2, S6, S15, S37, S42 and S51). K29 considered that an individual who had authorised the use of information for direct marketing should be entitled later to revoke that authorisation. Four submissions were opposed (L9, L10, L13 and L19) with two suggesting that the issue be addressed by code of practice (L17 and L22).

on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member states shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).”

A similar right exists in the Hong Kong privacy law.⁵⁴

- 2.9.15 Given the structure of our information privacy principles I take the view that this proposed new entitlement should be placed in principle 7 with details of any procedural aspects in Part V.



RECOMMENDATION 25

Information privacy principle 7 should be supplemented with a right to prevent the use or disclosure of personal information for the purposes of direct marketing through the deletion or blocking of personal information held by the agency for direct marketing purposes.

- 2.9.16 When a name is taken off a marketing list it should (if practicable) also be taken off lists held by agencies to which the details have been sold or traded. Indeed, complaints will often be made to a user of a list that has been rented from a list broker. It is important that requests to be taken off a list are also notified to the originator. Unless this is done the list information may be used again and again.
- 2.9.17 Existing principle 7(4) and (5) may have to be modified to ensure that renters or purchasers are obliged to notify the requests for deletion to the originator of lists. Principle 3(1)(g) will also oblige agencies which intend to use or disclose information for direct marketing to make the new entitlement under principle 7 known to individuals when collecting personal information from them .
- 2.9.18 I should add that I do not see deletion from mailing lists as being the complete answer to information privacy concerns in relation to direct marketing. If the existing principles were more rigorously applied by agencies the issues would tend to diminish on their own. In particular, agencies should be more open about the collection of personal information where it may be put to direct marketing purposes. The individual should be given an option to agree to this use or at the very least to object to it at the time of collection. Agencies should not portray the secondary use of personal information for marketing purposes as an implicit condition for obtaining goods or services.

2.10 PRINCIPLE 8 - Accuracy, etc, of personal information to be checked before use

- 2.10.1 Under principle 8 an agency must take reasonable care to check that personal information is accurate, up to date, complete, relevant and not misleading, *before* using it. The principle is modelled upon principle 8 in the Australian Privacy Act and is derived from the OECD “data quality principle”. This provides:

“Data quality principle

Personal data should be relevant to the purpose for which they are used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.”

- 2.10.2 Principle 8 also ties in with the obligation in principle 7 on an agency, of its

⁵⁴ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 34.



“Seminar participants are uniformly critical in the approach of the direct marketers.

The Privacy Act should create a right to be removed from a list as this will give people an alternative to proving that the addition of their name to a list was in contravention of any of the information privacy principles or public register privacy principles.”

- KATHRYN DALZIEL,
SUBMISSION S6

own initiative, to ensure the accuracy of information. Principle 7(2) provides:

“An agency that holds personal information shall ... on its own initiative, take such steps (if any) to correct the information, as are in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete and not misleading.”

2.10.3 Principle 8 is one of the shorter principles and is, I believe, easily understood. I am satisfied that the principle has worked satisfactorily in operation and this seems to have been borne out in consultation.⁵⁵

Meaning of “use”

2.10.4 In common with principle 10, principle 8 governs the “use” of personal information. There has been some speculation by commentators on the Act as to the meaning of “use” and, in particular, whether:

- the meaning is to be taken as the same as for principle 10;
- it might encompass disclosure;
- browsing information can constitute a use; and
- the process of verifying the accuracy of information itself constitutes use of that information.⁵⁶

2.10.5 On this last point Dr Paul Roth suggests that a way to avoid problems:

“would be to interpret the term ‘use’ in principle 8 in such a way that it does not apply to uses under principle 8 itself. That is, since principle 8 is aimed at the use of personal information without verification, where personal information is disclosed in order to verify its accuracy in compliance with principle 8 such a ‘reflexive’ use ought not to be caught.”⁵⁷

2.10.6 This would seem to be a plausible interpretation which could avoid interpretation difficulties in the utilisation of information for the purpose of verification, whether involving internal agency use or a use also entailing a disclosure.

2.10.7 This leads on to the question of whether an agency must check the accuracy of information when it is simply disclosing the information for use by someone else. The interests of individuals would obviously be harmed if an agency disclosed inaccurate information which was used to the detriment of the individual.

2.10.8 Other principles also bear on this issue in the sense that:

- pursuant to section 7(2) the agency may be obliged, of its own initiative, to take steps to correct information and to ensure that it is accurate having regard to the purposes for which the information may lawfully be used (and this does not appear to be limited solely to the use that the agency itself will make of the information);
- the recipient agency will be obliged in accordance with principle 8 to take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate etc.

However, it may be that under principle 7(2) the agency has taken no steps

⁵⁵ Ten out of 13 submissions agreed that principle 8 had worked adequately in operation (submissions K8, K9, K11, K13, K14, K18, K20, K25, K27 and K28). Submissions K12, K19 and K21 had some criticisms of the principle.

⁵⁶ A number of these issues are discussed in *Privacy Law and Practice*, paragraph 1006.42A.

⁵⁷ *Ibid*, paragraph 1006.42A.

as it had not itself contemplated using the information. Also, the recipient agency may have no feasible means to check the accuracy of the information.

- 2.10.9 The disclosure of personal information by an agency for use by someone else is one of the more significant actions that may affect the interests of an individual. Clearly it is undesirable for agencies to recklessly disclose inaccurate personal information without regard to the effect on the individual. It may be that the issue is satisfactorily addressed in our principles. It may be that principle 7(2) as it applies to the agency disclosing the information, and principle 8 as it applies to the recipient agency, together provide an appropriate response. It is also possible that principle 8 might be interpreted in such a way that the action of disclosure (or in a more limited basis the actions preliminary to a disclosure) constitute a “use” for the purpose of principle 8. Certainly there is a school of thought that takes a view that “use” for the purposes of principle 8 does not necessarily exclude the action of “disclosure” as is arguably the case for principle 10 (given that there is a separate disclosure principle 11). There has been no definitive Tribunal or court interpretation on the issue as yet. It may be desirable to make the position plain. A precedent is to be found in principle 3 of the Australian National Principles for the Fair Handling of Personal Information which states:

“An organisation should take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.”

- 2.10.10 It may be appropriate to amend our own principle 8 to read as follows:

“An agency that holds personal information shall not use *or disclose* that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.” [change highlighted]



RECOMMENDATION 26

Consideration should be given to amending information privacy principle 8 to substitute the phrase “use or disclose” for “use” in the first line.

2.11 PRINCIPLE 9 - Agency not to keep personal information for longer than necessary

- 2.11.1 Principle 9, which requires that an agency not keep information it holds for longer than is required for the purposes for which that information may lawfully be used, provides support to several of the other principles. The principle discourages agencies from continuing to retain personal information that is no longer needed. A privacy risk exists where such personal data is retained since:
- the information may become out of date and therefore should not be used (see also principle 8);
 - accumulations of personal information create a risk that they will be used regardless of the purpose for which the information was obtained or the ability to approach the individual directly for the same information (see also principles 2 and 11);
 - the retention of personal information well beyond its “use by date” represents an additional and avoidable security risk as it may inadvertently be disclosed (see also principles 5 and 11).

- 2.11.2 The present heading to principle 9 has caused misunderstanding. The princi-

“Principle 8 places an unfair burden on agencies who have been provided with information by a third party with whom the individual has primary contact. The agency that collects the information from the individual should be primarily responsible for ensuring that parties to whom that information is provided are notified of any material changes to the original data eg repayment of an outstanding debt.”

- BAYNET CRA,
SUBMISSION K21

ple 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.” I have recommended elsewhere that a simple reference to “retention of personal information” in the heading may suffice to avoid confusion.⁵⁸

Other jurisdictions

- 2.11.3 Although a retention principle is not found in all privacy laws, there are similar provisions in several. For example, principle 2(2) of the Hong Kong Personal Data (Privacy) Ordinance states:

“Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used.”

- 2.11.4 The 1993 Quebec Act Respecting the Protection of Personal Information in the Private Sector (section 12), states:

“Once the object of a file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned, subject to a time limit prescribed by law or by a retention schedule established by government regulations.”

- 2.11.5 The Australian Privacy Act does not currently have a principle corresponding to principle 9. However, the Australian National Principles for the Fair Handling of Personal Information include as part of a more general data security principle:

“An organisation should take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose”.⁵⁹

- 2.11.6 The UK Data Protection Bill provides at data protection principle 5 that:

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.”⁶⁰

Other enactments

- 2.11.7 Principle 9 is subject to the requirements of other enactments. There are, for example, laws requiring taxpayers to retain taxation records and health agencies to retain medical records. In the public sector the Archives Act and Local Government Act require the retention of certain archives.

- 2.11.8 Concerns have occasionally been expressed that over-zealous application of principle 9 might lead to premature destruction of records which may turn out in fact to be useful to the agency or individual and able to be used both lawfully and in accordance with the information privacy principles. The general answer to such a criticism is that the principle does *not* require premature destruction and in such circumstances an agency is able to adopt its own sensible approach to information and document retention. Furthermore, the principle does not oblige the *destruction* of information or documents, but simply obliges the agency no longer to “keep” information. It is possible, for example, for an agency to

⁵⁸ See recommendation 2.

⁵⁹ Australian Privacy Commissioner, *National Principles for the Fair Handling of Personal Information*, February 1998, clause 4.2.

⁶⁰ Data Protection Bill [HL] (UK), introduction version, schedule 1(I).

“Telecom questions the general need for principle 9. However, if it is to be retained then it should not be made more restrictive. Purposes for collection (and retention) of information change over time. It would be unduly restrictive to limit retention to the purposes for which the information was obtained in the first place.”

- TELECOM NEW ZEALAND,
SUBMISSION K12

return documents to the individual concerned or to disclose the information in accordance with principle 11 to an agency that does have a further lawful use for the information. It is possible that the marginal note, already mentioned, contributes to misunderstanding and I have already recommended that that be put right.

2.11.9 In consultation I asked whether principle 9 had led to inappropriate or premature destruction of documents. No evidence was produced of any real or significant problem in that respect. Some submissions speculated that such a risk might exist or asserted that destruction had occurred without giving any specifics. I do not believe that there is a significant problem although I acknowledge the possibility of employees misunderstanding the law and believing that they are obliged to destroy particular documents whereas in fact they are not.

2.11.10 It is possible that, motivated by principle 9, some documents have been destroyed in the last 5 years which were in fact required to be retained under the Archives Act until a disposal schedule had been agreed. If this indeed had happened it is, of course, regrettable but it needs to be understood:

- the actions of destroying such documents would have been based on a *misunderstanding* of the Privacy Act and not the requirements of the law itself;
- the root of any such problem is ignorance of agencies' responsibilities *under the Archives Act* rather than a problem with the Privacy Act.

2.11.11 This latter point raises a particular problem which has arisen in other circumstances as well. The Privacy Act operates as a kind of “overlay” on the actions of public sector agencies which are primarily governed by other legislation. The Act assumes compliance with the requirements of other legislation and, through section 7, provides that the principles defer to the requirements of other enactments. Problems can arise where employees in public sector agencies have not been made aware of agencies' obligations under other statutes. The issue arises not merely in respect of the Archives Act but also with the Official Information Act. The interaction with these pieces of legislation would work more satisfactorily if agencies were more aware of their other statutory obligations. Although the review of the operation of the Privacy Act can identify problems of this sort the solution may be primarily found elsewhere than in the Act or the operations of my Office.⁶¹ In my education and awareness functions in relation to the information privacy principles I do emphasise obligations under other statutes.⁶²

Requirement to retain information

2.11.12 Some people have suggested that individual privacy and personal autonomy can be harmed by premature destruction of personal information as well as its unnecessarily long retention. Examples might include:

- destruction by the sole repository of records concerning a person's origins (such as information about a birth parent in an adoption context or about the donor of gametes in relation to offspring born through assisted human reproduction);
- destruction of records so as to prevent the individual concerned exercising a right of access;
- destruction of records upon which a decision has been based so as to prevent any review of that decision or exercise of any judicial or administrative remedies (for example, records which might have indicated unlawful discrimination in an employment context).

⁶¹ Nonetheless my suggestion for amending section 7 may improve the situation. See paragraph 2.15 and recommendation 31(a).

⁶² For example, my Office released a compilation of materials relating to archiving issues in which the interaction with the Archives Act is canvassed. See Privacy Commissioner, *Compilation of materials in relation to the Privacy Act, Archives and Libraries*, 1995.

“The Department has strong concerns that documents are being destroyed prematurely, in breach of the Archives Act, on the basis that destruction is required by principle 9.”

- DEPARTMENT OF INTERNAL AFFAIRS, SUBMISSION K27

- 2.11.13 In New Zealand, some laws have tried to deal with this issue on a case by case basis. For example, the Health (Retention of Health Information) Regulations 1996 seek to ensure that medical records are retained to be available when needed through the imposition of a ten year minimum retention period. In other contexts, the issue has been addressed by creating statutory registers of certain key details which are always available to be accessed (such as exists with adoption information and has been proposed with respect to assisted human reproduction records).
- 2.11.14 The Freedom of Information and Protection of Privacy Act in British Columbia has tackled this issue directly in respect of the public sector. In a section entitled “Retention of personal information” it states:
- “If a public body uses an individual’s personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.”⁶³
- 2.11.15 A provision such as that has characteristics in common with the privacy rights and entitlements contained in information privacy principle 6 and Part V of the Act. It also has something in common with the entitlement that individuals have to obtain access to reasons for decisions affecting a person (a right which is currently found in section 23 of the Official Information Act 1982). That entitlement might well be considered a privacy right or entitlement and indeed it was initially intended to include such a right in the Privacy of Information Bill as an information privacy principle.⁶⁴ This would have replaced the Official Information Act provision. The primary reason for dropping the proposed principle was that its application would be limited to the public sector whereas the Privacy Act was intended to have a generally seamless application to both public and private sectors. That proposed entitlement, and I suggest the obligation to retain information under the British Columbia Act, have as much to do with expectations of procedural fairness in public agencies as with information privacy.
- 2.11.16 It would be problematic to have an obligation of the type in the British Columbia Act apply to all agencies in the public and private sectors. Submissions were almost evenly split on the question of reforming principle 9 to require the retention of information for a minimum period.⁶⁵ If such an obligation were to be applied to public sector agencies solely, I suspect that it would be better to link that obligation to section 23 of the Official Information Act than to the Privacy Act (although the merits either way could be further debated). The Archives Act may well achieve something similar in the public sector anyway.
- 2.11.17 I see the retention of information for minimum periods as a legitimate privacy issue but I suggest that a better way of addressing those concerns than amending principle 9 is through sector specific obligations. An example of this is the Health (Retention of Health Information) Regulations 1996. I have also recommended elsewhere that there should be an offence created where an individual destroys information after an access request is received in order to deny the individual’s entitlement to information (see recommendation 149).
- 2.11.18 To supplement these provisions I suggest that there should be a provision permitting a code of practice to require the retention of certain information or

“Specific minimum periods of retention should be judged on a case by case basis. These should be addressed by legislation or through guidelines dealing with specific issues as they relate to specific sectors. Retention time is not automatically linked to access opportunity. Knowledge of access to a record is a matter of education and information, and not time.”

- CONSUMERS’ INSTITUTE,
SUBMISSION K18

⁶³ Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 31.

⁶⁴ Privacy of Information Bill, principle 8.

⁶⁵ Eight submissions supported such a change (submissions K8, K11, K19, K20, K25, S24, S36, S42), 8 were opposed (K9, K12, K14, K18, K21, K28, K29, S11) with 3 neutral (K10, K13, K27).

documents. The requirement would be predicated on the possibility of individuals exercising their rights under the Act rather than directed towards any need by society for long term retention of documentation. Accordingly, I suggest that the power be limited to require the retention of information for a period not exceeding six years (which corresponds with the limitation period under the Limitation Act in most cases). The code making power would not be intended to be used to require long term records to be held on such matters as adoption or assisted human reproduction.



RECOMMENDATION 27

Section 46(4) should be amended to provide that a code of practice may require an agency to retain specified information or documents for a specified period, not exceeding six years.

2.12 PRINCIPLE 10 - Limits on use of personal information

2.12.1 Principles 10 and 11 give effect to the OECD “purpose specification principle” and “use limitation principle”. Limiting use and disclosure of personal information other than for purposes specified at the time of collection (or compatible purposes or those authorised by the individual concerned or by law) lies at the heart of any data protection law.

2.12.2 Principle 10 itself is straightforward and runs only to a single sentence. However, the detail is to be found in the list of 12 exceptions. Although principle 10 is an important, and central, principle I have no recommendations for amendment at this time. It appears to have worked satisfactorily albeit that there is often room for dispute as to precisely the purpose or purposes for which information was obtained.

Exceptions

2.12.3 Thirteen submissions responded to a question in the discussion paper asking whether the current exceptions to principle 10 are satisfactory or should be amended or any of them omitted. The submissions were almost equally split with seven submissions suggesting that the current exceptions are satisfactory⁶⁶ and six urging amendment.⁶⁷ No single pattern emerged from the submissions urging change although several did mention the individual authorisation exception as warranting amendments for example:

- to be more specific, for example requiring authorisation for a specific purpose;
- to be documented by being in writing;
- to spell out the elements of authorisation, for example being “free and informed consent”;
- to enable an individual to withdraw authorisation, for example by being taken off a mailing list.

2.12.4 Principles 2, 3, 10 and 11 presently include an exception where the individual concerned “authorises” the collection, use or disclosure of information by the agency. In recommendation 20 I propose that the individual authorisation exception be dropped from principle 3.

2.12.5 A key issue with such exceptions is whether the individual must positively indicate agreement to the departure from a principle or whether authorisation can be inferred from the circumstances. Commentators have suggested that the concept of authorisation is stronger than that of consent with the verb “authorise” more clearly denoting a positive and conscious act by the individual compared with “consent” where an act is being performed by another in relation to

⁶⁶ Submissions K14, K15, K19, K22, K25, K28 and K29.

⁶⁷ See submissions K11-K13, K18, K21 and F11.

“Exception (b) needs to be more specific, particularly to require authorisation for that other purpose specifically and in writing with free and informed consent with the onus being on the user to demonstrate the consent is free and informed.”

- AUCKLAND DISTRICT

COUNCIL OF SOCIAL SERVICE,

SUBMISSION K1.1

the individual concerned, who is in a passive position. On a complaint I have expressed my opinion that authorisation requires a positive act.⁶⁸

- 2.12.6 Even where a positive action is taken to give authorisation there sometimes remains a problem of specificity. Some agencies ask customers to sign authorisations, unlimited in time and subject matter, essentially purporting to authorise the agency to collect anything from anyone at any time and to use and disclose the information for any purpose to any person. Some might see this as attempting to contract out of some of the limitations imposed by the information privacy principles. Others may see collection of personal information by such means as “unfair” and in breach of principle 4.
- 2.12.7 All privacy laws have grappled with these issues. For example, article 7(a) of the EU Directive on Data Protection provides that personal data may be processed if the individual concerned “has unambiguously given his consent”. The Quebec Act Respecting the Protection of Personal Information in the Private Sector 1993 states in section 15 that:

“Consent to the communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.

“Consent given otherwise than in accordance with the first paragraph is without effect.”

- 2.12.8 In my view, the requirement for “authorisation” in the relevant exceptions to our principles is of similar effect to the concepts elaborated upon in Europe and Quebec. In the absence of any Tribunal or court decision suggesting otherwise I do not see the need to amend the Act to so provide. In terms of the submission suggesting that persons should be able to revoke an earlier authorisation enabling details to be used for direct marketing, I have made a proposal in respect of principle 7 to address this issue.⁶⁹ I have also canvassed the issue of “browsing”, which is relevant to principle 10, in the context of a proposal for defining the term “use”.⁷⁰

2.13 PRINCIPLE 11 - Limits on disclosure of personal information

- 2.13.1 Principle 11 gives effect to the OECD “purpose specification” and “use limitation” principles. Although some overseas laws combine the notion of use and disclosure into a single principle the New Zealand Act has discrete use and disclosure principles.
- 2.13.2 As with principle 10, the main point of discussion in respect of principle 11 concerns its exceptions rather than the basic principle of non-disclosure itself. Some aspects of principle 11 are explicitly or implicitly discussed elsewhere in this chapter, for example:
- the issues of individual “authorisation” arise in respect of principle 11 at least as much as with principle 10;
 - the direct marketing issues mentioned in respect of principle 7 and 10 are also issues under principle 11;
 - the saving of the effect of other statutes which authorise or require information to be disclosed is discussed in some detail in relation to section 7.⁷¹

⁶⁸ See case note 2976.

⁶⁹ See recommendation 25.

⁷⁰ See recommendation 16.

⁷¹ The requirements relating to section 7 are discussed at paragraph 2.15.

- 2.13.3 On this last point, it would be fair to say that some people have been confused as to the extent to which agencies can refuse to release information requested under the Official Information Act in reliance on principle 11. The position briefly stated is that if another enactment authorises or requires information to be disclosed this will prevail over principle 11 - see section 7(1). The Official Information Act is an enactment which may authorise or require information to be disclosed and therefore such requests should be dealt with in terms of that other statute rather than principle 11 (although, in appropriate cases, personal information may be withheld under that Act where necessary to protect the privacy of natural persons). My recommendation to transfer the substance of section 7(1) into principle 11 itself will, I believe, diminish misunderstanding on this score.⁷²
- 2.13.4 The discussion paper asked whether any of the exceptions to principle 11 should be amended or omitted. Twenty submissions were received with 13 suggesting amendment⁷³ and 7 submitting that the exceptions should be left alone.⁷⁴
- 2.13.5 There was no clear theme emerging from submissions advocating amendment. A number simply referred to their suggestions in respect of the exceptions to principle 10, particularly with respect to individual authorisation. One or two submissions expressly addressed matters that are dealt with in the Health Information Privacy Code 1994 which are therefore not particularly relevant to this exercise.

Disclosure for enforcement of foreign laws

- 2.13.6 The discussion paper also asked whether any new exceptions should be inserted into principle 11. Few submissions were received on this question with seven of the 12 submissions opposing the inclusion of new exceptions.⁷⁵ Five submissions advocated new exceptions.⁷⁶ Two of those submissions suggested that a new exception ought to be provided to enable the disclosure of information to law enforcement authorities to enable the maintenance of *overseas* laws.⁷⁷ This was in fact posed as a separate question which drew considerable support with eight submissions supporting the creation of such an exception,⁷⁸ two submissions opposing it⁷⁹ and three others offering observations.⁸⁰
- 2.13.7 The reason for raising the question of disclosure to overseas law enforcement agencies, is that the present exception provided in paragraph (e) in relation to the maintenance of the law is probably unavailable for such disclosures since it is linked to the notion of avoiding prejudice to the maintenance of the law by any “public sector agency” (which means a *New Zealand* public sector agency). This is likely to mean that the prejudice to the law covered may only be in relation to a *New Zealand* law. Accordingly, it is arguable that if disclosure is not otherwise permitted by principle 11, disclosures to overseas agencies to enable the investigation or prosecution of a foreign offence would only be permissible under the provisions of another enactment (such as the Mutual Assistance in Criminal Matters Act 1992).

- 2.13.8 Partly as a response to this issue, a specific provision was included in the Customs and Excise Act 1996. This permits the disclosure of certain specified

⁷² See recommendation 30.

⁷³ See submissions K7, K10-K13, K17-K19, K21, K29, S11, S19 and S25.

⁷⁴ See submissions K9, K14, K22, K23, K27, K28 and S13.

⁷⁵ See submissions K11, K13, K14, K18, K22, K23 and K28.

⁷⁶ See submissions K12, K19, K21, S11 and S15.

⁷⁷ See submissions K12 and S11.

⁷⁸ See submissions K3, K10-K13, K18, K21 and S11.

⁷⁹ See submissions K25 and S42.

⁸⁰ See submissions K19, K20 and K28.

“After some initial confusion, there have been few problems experienced by member services which can be traced to the Act itself. Difficulties appear mainly to stem from misapplication of the Act by those attempting to use it, or in some cases to hide behind it. This may suggest a need for greater emphasis on community education. The privacy principles have so far proved sound and realistic. Accessing training in the application of the Act has represented a considerable compliance burden for community organisations such as ours.”

- NZ FEDERATION OF FAMILY
BUDGETING SERVICES,
SUBMISSION S29

information from the NZ Customs Service to overseas customs organisations for certain defined purposes so long as the disclosure is pursuant to an agreement between the two customs organisations.⁸¹

- 2.13.9 In the discussion paper it was noted that the Nova Scotia Freedom of Information and Protection of Privacy Act 1993 might suggest a model if a new exception were to be warranted. That Act permits the disclosure of personal information:

“If the public body is a law enforcement agency and the information is disclosed ... to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.”⁸²

- 2.13.10 While there was support in the submissions for such a proposal there was also concern expressed that any such exception should be tightly controlled.⁸³ It was also suggested that it might be appropriate to limit the foreign agencies/countries to which it applies.⁸⁴ However, there was no submission from any affected law enforcement agency suggesting that there was a real problem to be addressed. None claimed that the principle was too restrictive or that the lack of other legislative authority for disclosure presented a problem for the maintenance of the law or cooperation with other law enforcement agencies. Indeed, the Ministry of Justice, the only core justice agency to make a submission on this question, did not unequivocally support such an exception but rather queried whether there was evidence of it being necessary. Mindful of the sensitivities surrounding enforcement information, and the exhortation in the OECD guidelines that exceptions to the principles should be “as few as possible” I am not inclined to recommend a new exception at this time. The matter could be reconsidered in the future if evidence of a problem emerges.

2.14 PRINCIPLE 12 - Unique identifiers

- 2.14.1 Principle 12 has some characteristics that set it apart from the other principles. For example, it does not mention “personal information” (although the definition of “unique identifier” refers to individuals and the identifier would constitute “personal information”). It also appears more prescriptive than some of the principles. This may have arisen by reason of the fact that the controls were not originally devised as a principle but as a clause in the original bill.⁸⁵

- 2.14.2 Although there is no direct equivalent of principle 12 in the OECD guidelines, other privacy laws and legislation place restrictions in relation to unique identifiers. For example, Australian and American privacy legislation place tight controls on the use of the tax file number⁸⁶ and Social Security Number.⁸⁷ The new UK Data Protection Bill proposes to allow the Secretary of State to prescribe special conditions in relation to any “general identifier”.⁸⁸ Controls on the use of the Identity Card Number and other personal identifiers have been imposed by code of practice under the Hong Kong privacy law.⁸⁹

⁸¹ Customs and Excise Act 1996, section 281. The provision requires consultation with the Privacy Commissioner.

⁸² Freedom of Information and Protection of Privacy Act 1993 (Nova Scotia), section 27(m)(ii). There would be no need, in the present New Zealand Act, to refer to “legislative authority” since this is already encompassed in section 7(1).

⁸³ See, for example, submissions K11, K13 and K18.

⁸⁴ See, for example, submission K13 and K19.

⁸⁵ Privacy of Information Bill, clause 108.

⁸⁶ Privacy Act 1988 (Australia), section 17 and Tax File Number Guidelines.

⁸⁷ Privacy Act 1974, USA, section 7.

⁸⁸ Data Protection Bill [HL] (UK), introduction version, Schedule 1, Part II, clause 4.

⁸⁹ Privacy Commissioner for Personal Data, *Code of Practice on the Identity Card Number and other Personal Identifiers*, Hong Kong, December 1997.

2.14.3 Principle 12 has taken a broad approach in seeking to address all unique identifiers, not simply specifically identified numbers. Principle 12 may thereby have the potential to be more effective than some overseas controls limited to a single identifier. Conversely, the principle's broad coverage may have extended its reach beyond the prime area of concern and may have caused unnecessary compliance difficulties.

2.14.4 Principle 12 has four parts to it. While having a degree of inter-relationship they each impose separate specific requirements, perhaps contributing to the perceived complexity of the principle - other principles tend to impose just a single requirement, or a couple of requirements, albeit sometimes accompanied by a series of exceptions of varying complexity. In fact, taken individually, the parts of principle 12 are relatively straightforward to understand and apply. Nonetheless, principle 12 appears to be the least well understood of the principles with many users of the Act perplexed as to its purpose and effect.

Rationale for principle 12

2.14.5 It is difficult to briefly encapsulate the underlying purposes of principle 12 in the way that one can for the other principles. Instead, there are a variety of concerns to which principle 12 is intended as a response. Dr Paul Roth has attempted to articulate the rationale for principle 12 in *Privacy Law and Practice*. He identifies the following features which I summarise:

- Principle 12 is in response to concerns about the accuracy and use of personal information where a unique identifier is assigned. In particular, the risk is that if one unique identifier is used for a wide variety of authentication and identification purposes in both the public and private sectors this would amount to a de facto universal identifier. De facto universal identifiers have been viewed as unsatisfactory because they are unreliable and a threat to individual privacy.
- Because a de facto universal identifier is not designed to be a true universal identifier it can be technically unreliable and vulnerable to falsification or error.
- Any unique identifier that facilitates the exchange and matching of personal information held by different agencies and within different record systems is perceived to be a threat to privacy. This may also lead to the socially undesirable practice of compiling composite profiles of individuals which may lead to any and every aspect of their lives being open to potential scrutiny by governments or private enterprise.
- The fear is that a de facto universal identifier emerging could ease the way towards the requirement of a national identity card or document. This brings with it a variety of concerns about inaccuracies and such like and the constraint on liberties. For some the idea of a national identity card is equated with the mechanisms of a Police State where identification can only be authenticated and entitlements made upon presentation of the card. Loss, lack or confiscation of such a card makes the individual a “non-person”.⁹⁰

2.14.6 Dr Roth concludes his characterisation of the rationale of principle 12 as follows:

“Accordingly, principle 12 is intended to promote data quality and impose an important form of control on the transfer and linking of individuals’ personal information. Principle 12(1) is intended to control the use of unique identifiers and define when it would be legitimate for an agency to assign them. Principle 12(2) controls the re-assignment of unique identifiers and thereby aids in promoting data quality and discourages illegitimate profiling and

⁹⁰ *Privacy Law and Practice*, paragraph 1006.65.

data matching of individuals. Principle 12(3) is directly concerned with data quality in that agencies must take all reasonable steps to verify the identity of individuals who are assigned unique identifiers. Finally, principle 12(4) controls the use of unique identifiers by restricting their use to the purposes in connection with which they were assigned, or a directly related purpose, and by requiring agencies not to require disclosure otherwise of unique identifiers. This is intended to discourage the illegitimate use of unique identifiers and their collection for linking or profiling purposes. It also individually promotes data quality, since restricting the spread of individuals' unique identifiers makes it less likely that incorrect, inaccurate or outdated personal information will later be used.”⁹¹

- 2.14.7 In addition to the points made by Dr Roth it might also be noted that:
- information matching rule 2 supplements principle 12 by prohibiting the use of unique identifiers in authorised information matching programmes except as provided in another enactment;
 - principle 12 inter-relates with the other eleven information privacy principles in so far as a unique identifier will be “personal information” and subject to the other principles;
 - the controls in principle 12 can supplement the objectives of various of the other principles, for example, principle 12(3) goes to the reliability of information, a matter also of concern in principle 8, while principle 12(4) touches upon the purposes for collection and disclosure of information, relevant to principles 1 and 11;
 - some individuals hold religious concerns about the process of numbering individuals. Others see the process as dehumanising (with the tattooing of concentration camp inmates as the most extreme example).

The meaning of “assign”

- 2.14.8 Each of the four clauses in principle 12 uses the term “assign”. That term is not defined in the Act and has sometimes caused confusion. The *Concise Oxford Dictionary* defines it as “ascribe or refer to”. However, it would not make the meaning any plainer to substitute “ascribe” for “assign”.
- 2.14.9 I have given consideration to including in the Act a definition of “assign”. Although the matter was raised in consultation no suitable definition has been suggested. I have concluded that it may instead be preferable to rely upon its ordinary English meaning and allow the meaning to be clarified over time in real cases. So far, there have been very few principle 12 complaints by which its meaning could be clarified and tested against real sets of circumstances. Most submissions did not favour attempting to define the term.⁹²
- 2.14.10 There are two main contexts in which agencies become confused as to whether an identifier has been “assigned”. The first is where the agency simply records the number on its files for later use but does not utilise the number to refer to the individual. An example is a bank which records the tax file number of an individual on the customer’s file. The number is not used for the bank’s own purposes in identifying the individual - it will have its own unique bank customer number - but for taxation purposes and to enable tax certificates to be printed which bear the identifier. In my view, this sort of arrangement will not generally constitute assignment since the number in the bank’s hands, in that scenario, probably does not even constitute a “unique identifier” (the defini-

“The Commission does not believe that the term ‘assign’ should be defined in the statute as it has a common meaning which is quite sufficient for the purpose of the Act.”

- STATE SERVICES COMMISSION,
SUBMISSION S11

⁹¹ *Ibid*, paragraph 1006.65.

⁹² See submissions K14, K19, K25, K28, S11 and S42. Submissions K11, K12 and K22 wished to see the term defined.

tion of unique identifier in section 2 requires the identifier to uniquely identify the individual in relation to the agency). Unless the bank has structured its data such that on being presented with the tax file number it can identify the customer in its records it has likely not assigned a unique identifier.

- 2.14.11 The second context for confusion is where there is a process for the generation of a set of numbers by a central agency which are allocated, often in batches, to agencies which may then utilise those numbers. The allocation process ensures that a particular number does not become available for allocation except on a single occasion. Such a process exists in relation to, say, the National Health Index (NHI) number in the health sector or the Law Enforcement Agency Reference Number (LEARN) in the justice sector. In my view, the mere generation of numbers is not sufficient to constitute assignment. Rather the identifiers need to be brought into effect in an agency for the purposes of uniquely identifying particular individuals. However, that has yet to be tested in a real complaint or Tribunal proceedings.

Limiting principle 12(2) to public sector unique identifiers

- 2.14.12 It may be argued that principle 12(2) goes further than necessary to meet reasonable privacy objectives and therefore possibly unduly causes compliance difficulties.
- 2.14.13 I consider that it is possible to limit the scope of principle 12(2) while still addressing the primary privacy concerns. Any increased privacy risk which might follow from cutting back its coverage can be compensated by a power to reassert the prohibition in particular circumstances by code of practice. The change would contribute to reducing compliance costs.
- 2.14.14 I consider that principle 12(2) could safely be limited to unique identifiers that are originally generated, created or assigned, by or on behalf of public sector agencies. If that change were to be made then both private and public sector agencies would continue to be prohibited from reassigning an unique identifier where the agency knows that the number had been assigned to an individual by a public sector agency. This would, for example, continue the prohibition on utilising the tax file number as a unique identifier but would mean that, for example, the problem which led to the Superannuation Scheme Unique Identifier Code 1995 would not arise.⁹³

- 2.14.15 Essentially this is what has been proposed in the Australian Privacy Commissioner’s National Principles for the Fair Handling of Personal Information. The Australian Privacy Act does not currently have a principle dealing with the assignment of unique identifiers but there has been a strong concern, particularly following the “Australia Card” debate, about the use of the tax file number. The proposed new principles are intended as suitable for the private sector and include the following principle on identifiers:

“7.1 An organisation should not adopt as its own identifier an identifier that has been assigned by a government agency (or by an agent of, or contractor to, a government agency acting in its capacity as an agent or contractor).

7.2 An organisation should not use or disclose an identifier assigned to an individual by a government agency (or by an agent of, or contractor to a government agency acting in its capacity as agent or contractor) unless one of paragraphs 2.1(d) to 2.1(h) applies.”

- 2.14.16 While there are no current “private” national unique identifiers it is conceiv-

⁹³ The Superannuation Schemes Unique Identifier Code 1995 could be revoked if this proposal is adopted.

“The Federation is of the view that rather than an attempt to define the word ‘assign’, it would be better for an advice booklet to give examples of ways in which the word is intended to apply. A definition would be unlikely to provide complete clarity.”

- NZ EMPLOYERS

FEDERATION, SUBMISSION K14

able that one might be devised, or arise through common usage. For example, there has been speculation that in the future individuals could be assigned with telephone numbers which they would carry throughout their lives. That in itself would not necessarily be a problem under principle 12(2) but if a wide range of agencies were to adopt the same number to identify the individual there would be an issue. This may be addressed by the Commissioner reimposing principle 12(2), in modified or unmodified form, to an identifier assigned by a private sector agency by way of code of practice.

- 2.14.17 There was little support in submissions for the proposal that principle 12(2) should be limited so that the prohibition is solely on the reassignment of numbers originally generated, created or assigned by a public sector agency.⁹⁴ Nonetheless, I consider the proposal is worthwhile.



RECOMMENDATION 28

In relation to the controls on reassignment of unique identifiers:

- (a) information privacy principle 12(2) should be limited so that the prohibition is solely in relation to the reassignment of unique identifiers originally generated, created or assigned by a public sector agency; and**
- (b) section 46(4) should be amended to make it clear that a code of practice may apply the controls in principle 12(2) to the assignment of unique identifiers generated, created or assigned by any agency (not simply a public sector agency).**

Enforceability of principle 12(2)

- 2.14.18 When the Privacy of Information Bill was introduced it provided for the making of regulations governing the creation and use of unique identifiers. The regulations would have prescribed offences carrying a maximum \$10,000 fine. The proposed provision was replaced by principle 12.
- 2.14.19 Principle 12(1), (3) and (4) are traditional data protection provisions for which the normal complaint and remedy process, focusing upon an individual's circumstances and the harm to that individual, fit satisfactorily. For example, it is conceivable that a complaint might be received and satisfactorily processed in the following circumstances:
- principle 12(3) - an agency fails to take all reasonable steps to ensure that unique identifiers are assigned to individuals whose identity is clearly established and as a result takes actions against a wrong individual;
 - principle 12(4) - an agency denies goods or services to an individual who refuses to supply a unique identifier in circumstances where the identifier should not have been demanded.
- 2.14.20 However, the complaints and enforcement procedures are unlikely to be effective in relation to the re-assignment provision in principle 12(2). In particular:
- re-assignment is likely to be done on a system-wide basis rather than on the individual basis upon which complaints normally arise;
 - it will often be difficult to show any particular harm or detriment for the action of re-assignment so as to constitute an "interference with the privacy of an individual" under section 66(1)(b). However, the re-assignment may be the key to future information sharing in breach of principles 2, 10 or 11, which cannot be proved (and may not even have been intended) at the time of re-assignment.
- 2.14.21 In consultation I asked whether the enforcement of principle 12(2) should be enhanced. Not many responses were received partly, I suspect, because many users of the Act find principle 12 perplexing or have had no real experience

"It is unlikely that actions of private sector agencies would create a common national identification number. If that situation did arise the Commissioner could address it by reintroducing a restriction through a code of practice."

- ASSOCIATION OF SUPERANNUATION FUNDS OF NEW ZEALAND, SUBMISSION K24

⁹⁴ Submissions K13 and K24 agreed with the proposal while 5 submissions disagreed - K11, K14, K18, K19 and K28. Other comments were received in submissions K12, S36 and S42.

with it. The responses were approximately evenly split with five submissions favouring an enhancement of the enforceability of principle 12(2)⁹⁵ with four opposed.⁹⁶

- 2.14.22 With the proposed limitation of principle 12(2) to identifiers assigned by public sector agencies it may well be appropriate to revert to an offence provision, the mechanism originally proposed in the bill. However, I am reluctant to depart from the civil law approach which underpins the Privacy Act's enforcement of the information privacy principles. I consider a preferable alternative to be modification of section 66 so as to remove the present harm or detriment requirement in relation to certain types of complaints involving principle 12(2).
- 2.14.23 I propose that individual complaints of a breach of principle 12(2) should continue to have to satisfy the existing requirements of section 66(1)(b) to constitute an "interference with the privacy of an individual" but that in certain circumstances proceedings be available for breach without having to prove harm or detriment of the type listed in section 66(1)(b). The circumstances I have in mind are where the re-assignment is "wilful" by which I mean cases for which compulsion or ignorance or accident cannot be pleaded as an excuse. The actions to be covered are those in which the assignment is intentional and deliberate notwithstanding the agency's awareness of the prohibition in principle 12(2). Such actions will almost certainly involve a continuing or on-going practice of assignment in breach of the principle. While damages could not be awarded, an order could be made by the Complaints Review Tribunal in relation to continuing or repeating the interference.



RECOMMENDATION 29

Section 66(1) should be amended so that an interference with privacy may be established notwithstanding the absence of any harm or detriment of the type set out at section 66(1)(b) in cases of wilful breach of information privacy principle 12(2).

2.15 SECTION 7 - Savings provision

- 2.15.1 Section 7 is a savings provision. In effect, it provides that the Privacy Act is subject to the provisions of any other enactment (which includes regulations) dealing with a matter which would otherwise be determined solely by reference to the information privacy principles. Moreover, an action will not constitute a breach of principles 1-5, 7-10 and 12 if that action is authorised or required by or under law. Section 7 essentially recognises specific public interests contained in a variety of other enactments and provides for their continuation, and recognition, under the Privacy Act.
- 2.15.2 While there might have been some benefit in having a Privacy Act which did override other legislation in terms of certainty of the rules in relation to personal information, there would have been considerable, and understandable, opposition from those organisations already applying their own regime under specific legislation. Much research would have been required to identify all legislation which might include provisions covering information issues of the time the Privacy Act was passed. Parliament decided to meddle with existing legislation as little as possible.
- 2.15.3 It may be acknowledged here that international human rights treaties allow rights to be limited so long as the limits are set out in law. This provides for certainty and transparency. It also permits limited and justified departures from the expected rights, when made democratically.

⁹⁵ See submissions K11, K13, K19, K21 and S11.

⁹⁶ See submissions K14, K18, K23 and K28.

2.15.4 By way of contrast with the New Zealand position it may be of interest to know that many Canadian provinces have provisions in their privacy legislation which provide that their privacy law will override a subsequent general Act unless the latter Act is expressly provided to prevail notwithstanding the privacy legislation.⁹⁷

Subsections 7(1) to (6)

2.15.5 Section 7 is a key, but rather complicated, provision which essentially provides that all other legislation (both statutes and regulations) will override the principles identified in the various subsections on specified matters. It is particularly unusual to allow regulations to override an Act. The normal rule would be that Acts have priority over regulations.

2.15.6 Section 7(1) provides that a specific provision in another *enactment* (that is, act or regulation) authorising or requiring personal information to be made available will override principles 6 (access to personal information) and 11 (limits on disclosure of personal information).

2.15.7 Section 7(2) provides that a specific provision in any *Act* prohibiting or restricting the availability of personal information, or regulating the way in which personal information may be obtained or made available, will override principles 6 and 11.

2.15.8 Section 7(3) applies the same regime as subsection (2) to provisions in *regulations*⁹⁸ but complicates the situation by limiting its application to regulations in force before the Official Information Act was passed in relation to the public sector, regulations in force before the Local Government Official Information and Meetings Act was passed in relation to local authorities, and regulations in force before the Privacy Act was passed in relation to any other agencies.

2.15.9 Section 7(4) provides that an action done will not be a breach of any other of the principles other than principles 6 and 11 if that action is authorised by “or under law”.

2.15.10 Section 7(5) provides that nothing in principle 7, which concerns correction of personal information, applies in respect of any information held by the Department of Statistics where that information was obtained pursuant to the Statistics Act 1975.

2.15.11 Finally, section 7(6) provides, subject to the provisions of Part VII, nothing in any of the information privacy principles is to apply in respect of a public register. This provision is discussed in relation to section 60 where a recommendation for reform is made.⁹⁹

Simplifying the savings regime

2.15.12 The existence of section 7 is critical to understanding the present regime for the interaction between the information privacy principles and other laws. Unfortunately, ignorance concerning its existence and effect has sometimes led to

⁹⁷ See, for example: An Act Respecting the Protection of Personal Information in the Private Sector, 1993 (Quebec), section 94; An Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information 1982, (Quebec), sections 168 and 169; Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 78. The British Columbia Act provides that “if a provision of this Act is inconsistent or in conflict with a provision of another Act, the provision of this Act prevails unless the other Act expressly provides that it, or a provision of it, applies despite the fact”.

⁹⁸ Only regulations made by Order in Council are covered. A problem has arisen in respect of the Status of Financial Reporting Standards which are regulations for the purpose of the Regulations (Disallowance) Act but are not issued by Order in Council.

⁹⁹ See paragraphs 7.8.1 - 7.8.15 and recommendation 92.

difficulties in the operation of the legislation. The typical problem involves an agency which believes that it is unable to utilise information in a particular way because it is not permitted by an information privacy principle. Such agencies are sometimes unaware, or purport to be unaware, that the action may well be permitted by other legislation which authorises or requires it.

2.15.13 If one accepts the basic proposition that the information privacy principles should be overridden by other specific laws, as I do, then section 7 can probably be seen technically as a satisfactory and effective provision. Unfortunately, the provision cannot be fully effective unless its content is known to the persons who must apply the principles, particularly agencies which hold information which is subject to other laws. My suggestions for improving the position in that regard involve:

- a new marginal note;
- dispersal, where appropriate, of some elements of section 7 into the relevant information privacy principles;
- simplification of section 7.

I also make some suggestions for modest substantive changes to section 7 to enhance privacy rights while simplifying the position at the same time.

Marginal note

2.15.14 I have recommended elsewhere that the marginal note should be made more informative given that many people working with the Act are not familiar with technical statutory terms such as “savings”.¹⁰⁰ I suggest that the marginal note should be altered from “Savings” to “Saving of effect of other laws” or “Effect of other laws on information privacy principles”.

Dispersal of elements of section 7

2.15.15 Persons who frequently use the Privacy Act realise the importance of section 7 and generally do not have too many difficulties with it. However, less familiar users, particularly those who have a copy of the information privacy principles but not the other parts of the Act, are sometimes unaware that the principles are not the last word on the subject of collection, use and disclosure of personal information, and must be read subject to other enactments. This is not apparent from reading the principles themselves. It is necessary to read section 7. People unaware of section 7 have sometimes wrongly suggested that the principles fail to acknowledge public interests which compete with privacy. I suggest that parts of section 7 be dispersed to form part of the principles to which they relate. On this basis agencies and their staff will have a better picture of the effect of the principle when reading the principle alone.

2.15.16 There is a downside to dispersing elements of section 7 into the principles. In particular the principles will expand in length. It is fair to say that section 7 was adopted as a mechanism to avoid cluttering the various principles with repeated lengthy exceptions saving the effect of other laws. However, I think the proposal for dispersal need only modestly increase the length of the principles.

2.15.17 My proposal for dispersal of sections 7(1), 7(4) and 7(5) involves transferring elements of the following subsections into the relevant principles:

- section 7(1) - transfer into principle 11 (the aspect concerning principle 11 only);¹⁰¹
- section 7(4) to be transferred into principles 1 to 5, 7 to 10 and 12;
- section 7(5) which relates to a single law and a particular agency, should not be transferred into a principle but should instead remain in section 7 or be placed with the exemptions in Part VI.

¹⁰⁰ See recommendation 2.

¹⁰¹ The aspect of section 7(1) concerning principle 6 may remain where it is.

2.15.18 In the context of section 7(1), the official information statutes are the main enactments which authorise or require personal information to be made available. They also seem to be the statutes most overlooked by public sector staff receiving a third party request for someone’s personal information. A number of submissions considered that section 7 should make clear how the effect of the Official Information Act is saved.¹⁰² Accordingly, in transferring the elements of section 7(1) into principle 11 thought should be given to referring to those statutes. Indeed, this was the approach taken in the disclosure principle in the Privacy of Information Bill which contained an exception relating to where:

The disclosure is made pursuant to any provision of the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987.¹⁰³

2.15.19 The select committee dropped the exception and, in effect, incorporated it into the more general savings provision, section 7(1). While the legal effect is the same, the experience of the last five years suggests that public understanding might have been enhanced by remaining with the original drafting. If the exception were to be reinstated it could, instead of simply mirroring section 7(1), provide something along the lines of the following:

That the disclosure is made pursuant to a provision of the Official Information Act 1982, the Local Government Official Information and Meetings Act 1987 or any other enactment that authorises or requires personal information to be made available.¹⁰⁴

This will strengthen knowledge of the Official Information Act and Local Government Official Information and Meetings Act which is not well understood by all public sector employees.



RECOMMENDATION 30

Section 7(1) should be amended by transferring its content, in so far as it relates to information privacy principle 11, into principle 11 as a new exception.



RECOMMENDATION 31

Consideration should be given to transferring the content of:

- (a) section 7(4) into information privacy principles 1 to 5, 7 to 10, and 12 as exceptions; and**
- (b) section 7(5) into Part VI.**

2.15.20 Several provisions in section 7 touch upon the access rights arising from information privacy principle 6. The place where users of the Act will expect to see provisions allowing for withholding information is Part IV which sets out the good reasons for refusing access to information.¹⁰⁵ Accordingly, the content of section 7(2) and 7(3), in so far as they relate to principle 6, should be transferred into a new section to appear in Part IV, perhaps as section 29A.

2.15.21 This was the approach that was taken in the Privacy of Information Bill prior to

¹⁰² See submissions M1, M4, M7, M10, M13, M17, S1, S19, S20, S31 and S42. Submissions M8, M16 and S11 saw no need for change in this regard.

¹⁰³ Privacy of Information Bill, principle 14(1)(d).

¹⁰⁴ A similar approach could be taken to the transfer of elements of section 8(4) into principle 9 by making special reference to the Archives Act.

¹⁰⁵ Although some aspects of these subsections might be said to belong in Part V (such as section 72(2)(b)), it will be simpler to place all the material in Part IV.

“The effective interaction of the Official Information Act and the Privacy Act is crucial in terms of day to day access to information held by the public sector. We are aware of requests for information being made of Government departments which are refused on the grounds of the Privacy Act meaning the journalist concerned has to make the request again under the Official Information Act. Clearly Government officials are unsure of the boundary between the two statutes.”

- COMMONWEALTH PRESS UNION
SUBMISSION M13

the select committee’s decision to bring all the savings provisions affecting the information privacy principles together into section 7.¹⁰⁶ I believe that it will make more sense for people who must work with the Act, and apply it to requests for information, to have this provision located in Part IV, to which reference is expressly made in principle 6, than in section 7. Indeed, to treat the provision very much like the other reasons for refusal set out adjacent to section 29 will somewhat dispel the fiction perpetrated by section 30 that refusal is not permitted for any other reason than those set out in sections 27 to 29. If this proposal is adopted a resultant amendment will also need to be made to section 30.



RECOMMENDATION 32

The content of section 7(2) and (3), in so far as they relate to information privacy principle 6, should be relocated into Part IV.

Sections 7(2) and (3) as they concern principle 11

- 2.15.22 Principle 11 prohibits the disclosure of personal information subject to exceptions. It is not a principle which actually authorises the release of information which is otherwise prohibited or restricted. Nor does principle 11 have anything to say about the manner in which personal information may be obtained or made available. It might therefore seem that if subsections (2) and (3) omitted any mention of principle 11 there might be no change in effect - one might continue to say that principle 11 did not derogate from any Act or regulation which does the things specified in those subsections.
- 2.15.23 It has been suggested that the reference is included merely out of caution so as to ensure that there is no misunderstanding on the point. Supporters of this view would suggest that the reference to principle 11 is intended to give comfort to agencies which hold information which may be subject to other enactments that those laws continue to have effect. If that is the sole objective I believe that it has been rather confused by unnecessarily combining the provision with principle 6.
- 2.15.24 The position would become clearer if the principle 11 and principle 6 provisions were to be disentangled. This will occur if my recommendation is accepted to transfer the content of the section 7(2) and (3), in so far as they relate to principle 6, into Part IV of the Act. However, even if that material is not relocated, there will still be some benefit in disentangling the provisions so as to make their effect clearer.
- 2.15.25 The provision, in so far as it relates to principle 11, has been derived from a much clearer provision in the Privacy of Information Bill. The disclosure principle in the bill originally provided, before the material was amalgamated into section 7, that:
- “(2) Nothing in subclause (1) of this principle shall be taken as authorising the disclosure of any personal information in any case where the disclosure of that personal information would be a breach of any obligation of secrecy or non-disclosure imposed by the provisions of any enactment.”¹⁰⁷
- 2.15.26 The importance or potential of such a provision becomes clearer in that form. Expressed in the original manner the provision does not simply save the effect of other laws but also clearly precludes an agency from relying upon an exception to the disclosure principle in a case where a secrecy or non-disclosure provision constrains disclosure beyond what would otherwise be permitted. This

¹⁰⁶ Privacy of Information Bill, clause 32.

¹⁰⁷ Privacy of Information Bill, section 8, principle 14(2).

would appear to mean that an interference with privacy involving a disclosure of personal information may encompass a disclosure outside the bounds of principle 11 as restricted by the provision of another statute. This, to my mind, is a desirable state of affairs if Parliament's will in enacting secrecy or non-disclosure provisions, are to be given effect to and individual privacy respected.

- 2.15.27 For example, say a statutory health agency is obliged by a provision in an enactment to protect sensitive medical information on a database that it operates and not to disclose the information except to, say, a single statutory official. It transpires, on a complaint, that the information was disclosed in identifiable form in breach of the enactment to drug companies, politicians or researchers. In such circumstances, the original formulation that appeared in the Privacy of Information Bill would preclude the agency from seeking to argue that the disclosure was a “directly related purpose” or for “research purposes” etc.
- 2.15.28 The issue has been examined in Australia by a committee of the House of Representatives which had inquired into the protection of confidential information held by the Commonwealth Government.¹⁰⁸ That report noted that information privacy principles 10 and 11, which are similar to our own, set a weak minimum standard that is largely inadequate for confidential information. The Standing Committee stated:

“The Committee agrees where specific legislation contains express secrecy provisions the Privacy Act should not be used to expand the access that is otherwise permissible. To do so would undermine the protections expressly provided by the secrecy provisions and would allow a distortion of the protected purpose of the Privacy Act.”¹⁰⁹

The Committee recommended that the Australian Privacy Act be amended to provide where an Act other than the Privacy Act deals expressly with a matter of permissible use and disclosure, information privacy principles 10 and 11 do not operate to provide additional grounds for disclosure.

- 2.15.29 In my view, this is essentially what the original provision in the disclosure principle in the Privacy of Information Bill would have achieved. It appears that without necessarily intending to depart from that objective, the matter has become confused through its transfer into section 7 and amalgamation with a savings provision concerning principle 6. In my view, the matter is best resolved in relation to principle 11 by:
- disentangling the principle 11 issues from the principle 6 issues in section 7(2) and (3);
 - dealing with the effect of secrecy or non-disclosure provisions in all enactments identically and not distinguishing between statutes and regulations;
 - drafting the provision in a straightforward manner whereby its effect is plain; and
 - transferring the brief resulting provision into principle 11 itself so that its existence will more readily be brought to the attention of users of the principle.
- 2.15.30 It appears to me that the objective can be readily achieved by simply reverting to the formulation used in the Privacy of Information Bill.

¹⁰⁸ House of Representatives Standing Committee on Legal and Constitutional Affairs of the Parliament of the Commonwealth of Australia, *In Confidence: A Report of the Inquiry Into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth*, June 1995

**RECOMMENDATION 33**

Section 7(2) and (3), in so far as they relate to information privacy principle 11, should be repealed and replaced with a single provision, which may be relocated into principle 11 itself, to the effect that where another enactment imposes a more restrictive obligation of secrecy or non-disclosure than principle 11, the principle does not operate to provide additional grounds for disclosure.

- 2.15.31 Section 7(2) and (3), once the material concerning principle 11 has been omitted, may simply be transferred into Part IV or may remain within section 7. However, I suggest that consideration ought to be given to restricting the effect of section 7(3) so as to increase the access rights of individuals.
- 2.15.32 When the Official Information Act 1982 was introduced it was a significant freedom of information inroad, preceded only by the Wanganui Computer Centre Act 1976, into a general regime of secrecy under the Official Secrets Act 1951. It was therefore quite understandable that a cautious decision was taken to save the effect of restrictive provisions in other enactments which were more narrowly focused than the all embracing Official Secrets Act. However, it was recognised that a culture of “open government” could be set back if a series of new restrictions could be introduced by regulation. Accordingly, while the effect of all other statutes was saved, only those regulations in force when the Official Information Act commenced were saved. The Danks Committee stated:

“As we have already mentioned there are, aside from the Official Secrets Act, many other statutes which provide protection for specific areas of information as well as sanctions for unauthorised disclosure. It is not uncommon for protection clauses to be included in new enactments. One result the Committee would not wish to see arising from the changes recommended in this report, would be a rash of new protective measures. This would, we consider, seriously undermine the Government’s intention and we hope it can be resisted. *The compatibility of protection accorded by existing statutes with proposals we are developing should be reviewed in due course.* This review will be part of the work programme of the new machinery we are proposing.”¹¹⁰

- 2.15.33 A review of statutes was part of the work programme of the Information Authority although there has been some criticism of the limited scope of the actual work undertaken (extending, for example, solely to enactments affecting “official information” as that term was then used in the Official Information Act and therefore not extending to the full range of information held by public bodies subject to the official information statutes following the 1987 extensions).

Restrictions on access in regulations

- 2.15.34 For the last 15 years the Executive has been constrained from creating new withholding provisions by regulation. The basic prohibition as it applies to information held by government departments was since extended in 1987 to other parts of the public sector and to local government. Since 1993 there has been a constraint upon using regulations to provide further reasons to withhold information which is held in the private sector. In my view, it is timely to consider removing regulations as a reason for refusing personal access requests.
- 2.15.35 My proposal is that a sunset clause provide that section 7(3) will expire after three years. The three year period would allow affected agencies, if they wished, to:
- identify any provisions in regulations upon which they rely to withhold infor-

¹⁰⁹ *Ibid*, page 64.

¹¹⁰ Committee on Official Information, *Towards Open Government: General Report*, 1980, page 28.

- mation where there is no corresponding reason for refusal in Part IV; and
- consider whether the provision continues to be necessary and, if so, for equivalent provision to be made in primary legislation.

There would be no need to review the entire series of regulations in my view. Departments which know that they rely upon the regulations may review their options. Others will, I am sure, be quite able to operate without section 7(3), just as they do with post-1993 regulations.

- 2.15.36 Consultation did not bring forward any instance of regulations which are relied upon by agencies pursuant to section 7(3) in circumstances where withholding under Part IV would not be possible.¹¹¹ Nor have any complaints been brought to me concerning circumstances in which reliance has been placed upon section 7(3).
- 2.15.37 The regulations in issue, particularly those relating to section 7(3)(a)(i), were made at a time in which there were no relevant enforceable rights of access to personal information. In other words, they were crafted prior to the emphasis upon “open government” and accountability, in information terms, to the individual about whom information is held. It is desirable, in my view, that the public policy underpinning them as authority for refusing access should be reconsidered in today’s environment.
- 2.15.38 I see my proposal as being in keeping with the continuing review envisaged by the Danks Committee and the notion espoused in the Official Information Act of “increasing progressively the availability of official information to the people of New Zealand.”



RECOMMENDATION 34

A sunset clause should provide for the expiry of section 7(3) after a period of 3 years.

Restrictions on access in other statutes

- 2.15.39 Secrecy provisions are a traditional matter of concern for anyone interested in laws governing access to information. For example, the Information Authority made a study of them in the 1980s and, more recently, a similar review of secrecy provisions was carried out in respect of all statutes in Queensland.¹¹² I could not complete discussion of section 7 without noting that there continue to be certain statutory secrecy or non-disclosure provisions, the effect of which is saved by section 7(2), which appear to be unnecessarily restrictive when it comes to an individual exercising their rights of access under principle 6.
- 2.15.40 Secrecy or non-disclosure provisions in statutes and regulation have a role notwithstanding that the Official Information Act and Privacy Act deal with many information access and disclosure matters. For example:
- a statutory non-disclosure provision may be necessary so as to deny access to a class of documents or information in the event of an access request under the Official Information Act - although it is, of course, essential that such provisions be enacted sparingly and only in appropriately justified circumstances. Otherwise the integrity of the access entitlements under that statute will be eroded;
 - to constrain, consistent with public policy, the disclosure of particular types of information by agencies or employees of agencies;
 - to enable an agency to withstand a demand from another public agency - for example, enabling individual tax records to be held off limits to statutory requisitions from other departments or from Ministerial requests.

¹¹¹ Although some submissions asserted that relevant regulations may exist. See submissions M11 and S20.

¹¹² Queensland Law Reform Commission, *Freedom of Information Act 1992: Review of Secrecy Provision Exemption*, March 1994.

- 2.15.41 While I certainly accept the case for secrecy or non-disclosure provisions in appropriate circumstances, the provisions are often expressed in such a broad fashion that they sometimes unintentionally oust rights of access by the individual concerned. Often the need which led to the enactment of a secrecy provision had nothing to do with denying access to personal information by the individual concerned but that can be the effect. In my view, the tax legislation is an example of this. There is a very strong case for there to be a secrecy provision in the Tax Administration Act. However, I am not convinced of the need for that to be written in such a way as to deny an individual's right of access to information held about him or her.¹¹³ Another example is the secrecy provision which applies to the Police Complaints Authority. I have been concerned at a recent case which has the effect of allowing that secrecy provision to effectively deny individual access to a class of information.¹¹⁴ I accept that there will be many cases in which both the IRD and the Police Complaints Authority will, entirely appropriately, withhold information from a requester. However, the withholding grounds in the Privacy Act are, in my view, quite sufficient to achieve that purpose. My concern is that the secrecy provisions unnecessarily oust the access regime including independent review of a decision to withhold.¹¹⁵
- 2.15.42 Departments which administer statutes containing secrecy provisions should consider whether they ought to be reviewed so that the effect on individual access requests (as against Official Information Act requests) are not unnecessarily precluded. For the most part, this could be achieved by including an exception in the secrecy provision allowing disclosure to the individual concerned. In other cases, where it is intended that certain classes of information be withheld from the individual concerned, this may be provided in a way that the individual access entitlements continue for the balance of information held.

The rump of section 7

- 2.15.43 Section 7 has a central place in the present scheme of the Act. With the changes that I have recommended it will become a much smaller and less important provision. However, there also remains the possibility that some of my recommendations will be acted upon and not others. I have deliberately presented the suggestions in a manner whereby it is possible to avoid an "all or nothing" choice. It may therefore be useful to briefly mention what might be left of section 7 when most or all of my recommendations are taken into account.
- 2.15.44 Section 7 will roughly appear as follows:
- section 7(1):
 - as it relates to principle 6, retained as it is;
 - as it relates to principle 11, omitted, with the content transferred as an exception into principle 11;
 - section 7(2) - omitted, with the content distributed as follows:
 - as it relates to principle 6 - transferred into Part IV as a reason for refusing a request for access;
 - as it relates to principle 11, combined with relevant material from section 7(3), and transferred in redrafted fashion to principle 11;
 - section 7(3) omitted, and transferred as follows:
 - as it relates to principle 6, into Part IV together with section 7(2);
 - as it relates to principle 11, combined with section 7(2) as a

¹¹³ I have taken up these concerns in my Report to the Minister of Justice on Clause 81 of the Tax Administration Bill, October 1994.

¹¹⁴ See *Attorney-General v The District Court at Nelson*, 29 June 1998 (CA215/97).

¹¹⁵ Albeit that the exercise, or non-exercise, of the discretion to disclose may be a matter amenable to review by the courts or Ombudsmen.

new part of principle 11 or as a part of section 7 disentangled from access issues;

- section 7(4) omitted, by variously dispersing the provision as exceptions to the relevant principles or, on a more modest reform, by dispersing some of the content as exceptions and retaining the balance in section 7;
- section 7(5) retained in section 7 or alternatively relocated with the specific exemptions found in Part VI;
- section 7(6) - omitted, by transferring a redrafted provision into section 8.

2.15.45 Depending upon what material is retained a suitably descriptive new marginal note may be adopted.

2.16 SECTION 8 - Application of information privacy principles

2.16.1 This section provides for the application of the information privacy principles. Subsections (1) to (3) set out the application of principles 1 to 11 to information collected or obtained before or after the commencement of the Act while subsections (5) and (6) set out the application of principle 12 to unique identifiers assigned before or after the Act's commencement.

2.16.2 Subsection (4) provides that nothing in principle 3 applied to the collection by means of a printed form so long as the form was printed before the commencement of the Act and was used before 1 July 1995. This was one of the measures to phase in the requirements of the Act in order to minimise compliance costs and disruption to businesses.

2.16.3 The provision has been considered in a Complaints Review Tribunal case but has not caused any difficulty in operation.¹¹⁶

2.17 SECTION 9 - Postponement of application of principle 11 to lists used for direct marketing

2.17.1 Section 9, like section 8(4), assisted in the phase-in of the application of the Act. It allowed the continued disclosure by direct marketers of personal information, particularly names and addresses, on existing lists until 1 July 1996, without having to obtain the authorisation of the individuals concerned. This provided a “breathing space” whereby direct marketers could, for example, contact individuals on such lists and inform them of their options, such as to remain on the list or to be removed, to begin the construction of brand new lists in conformity with the collection principles.

2.17.2 I believe that the provision was successful in easing the position of direct marketers enabling them to make the transition from “anything goes” to one in which complaints could be brought under the new law. The transitional provision was appreciated by the practitioners of direct marketing and list brokers. It provided an opportunity for the NZ Direct Marketing Association to inform its membership as to the requirements of the new Act and to assist in compliance programmes.

2.17.3 One unfortunate misunderstanding, which was not entirely dispelled by the active efforts of the NZDMA in training, was that direct marketers were somehow exempted from the Privacy Act until 1 July 1996. It is plain that the section only has relevance to principle 11 and, for example, the collection principles applied from the commencement of the Act as with other agencies. It remains a disappointment to me that there continues to be considerable non-compliance, or only partial compliance, with agencies collecting personal information for direct marketing purposes. Competing priorities have prevented

¹¹⁶ *Powell v Special Education Service*, Complaints Review Tribunal, 26 July 1996, CRT Decision No. 26/96.

me from undertaking compliance monitoring work in this area but the NZDMA has made positive efforts to encourage compliance.

2.18 SECTION 10 - Application of principles to information held overseas

- 2.18.1 Section 10 provides that information held by an agency includes information held by that agency outside New Zealand. For the purposes of principles 5, 8, 9, 10 and 11, the information in question must have been transferred out of New Zealand. For the purposes of principle 6 and 7, all personal information, whether or not it was transferred out of New Zealand, is covered. An immunity is extended to breaches of the information privacy principles outside New Zealand that result from an agency's compliance with foreign laws.
- 2.18.2 The provisions seek to prevent non-compliance with the information privacy principles by agencies that might be tempted to move their holdings of personal information overseas. This is relevant to the problem of so-called "data havens". It is possible that section 10 also offers some reassurance to countries transferring personal information to New Zealand that any further transfer on to a third country will not deprive the information of the Privacy Act's safeguards. However, the section does not adequately deal with the problems of the transfer of New Zealanders' information to data havens nor the routing of personal data through New Zealand on to another agency in a data haven. I mention these issues below in the context of a proposal directed to controls on transborder flows of personal information.
- 2.18.3 However, section 10 also has a far more mundane objective which has nothing to do with concerns about agencies which would deliberately transfer information into a jurisdiction without privacy laws so as to avoid the controls of the Act or any other data protection law. Rather, it is a fact of life that some businesses operate across national boundaries and, without any wish to circumvent the law, may move information overseas to use or process it. A current example concerns the position of banks operating in New Zealand. Nearly all banks are now foreign owned and several of these have their head office in Australia, a jurisdiction having no general privacy laws covering the private sector.¹¹⁷ It has been reported, for example, that the Bank of New Zealand is relocating its data processing centres to Melbourne.¹¹⁸ While the information remains held by the BNZ section 10 requires that the information must be held securely as required by principle 5 and held, used and disclosed only in accordance with principles 8 to 11. It also means that BNZ customers can continue to exercise their rights of access and correction under principles 6 and 7. It does not cover information disclosed to, and thereafter held by, another agency in Australia in a way which would give remedies to a New Zealand customer who may be affected.

Transborder data flows

- 2.18.4 I have come to the conclusion that section 10 alone is not adequate for dealing with issues of "data export" or "transborder data flows". In making a proposal for change I have carefully considered the international dimension, particularly the OECD guidelines and also New Zealand's position as a "third country" in respect of the EU Directive on data protection. I have also been mindful of the fact that transborder data flows have been an issue in a variety of ways during the last five years and this may increasingly be the case. For example, transborder data flows issues have arisen in a variety of my functions such as:
- responding to enquiries - for example, recent public concerns at the sale of

¹¹⁷ Part IIIA of the Privacy Act 1988 (Australia) will apply to Australian banks as "credit providers". However, that Part is not equivalent to a general privacy law but has relevance only to some aspects of credit reporting by credit reporting agencies.

¹¹⁸ "BNZ Data Processing Goes Offshore," Infotech Weekly, The Dominion, 31 May 1998.

large quantities of valuation data to a company in Queensland;¹¹⁹

- my complaints function - for example, involving the transfer of a man's HIV details to a Pacific Island country resulting in adverse action against the individual;¹²⁰
- examining legislative proposals - for example, I have formally reported to the Minister of Justice in respect of transfer of information pursuant to the Passports Act and Trans-Tasman Mutual Recognition Act and have examined legislation for the transfer of customs information to overseas agencies;¹²¹
- my code of practice function - I have imposed some relevant controls in the context of the privatisation of the Government Computing Service which was responsible for data processing in respect of the law enforcement and taxation systems.¹²²

I also received a number of submissions during consultation on this review on the subject of transborder data flows.¹²³

- 2.18.5 In the material that follows I outline the international approach, and the approach taken in several jurisdictions, to the question of transborder data flows. I then make a proposal for how the matter might appropriately be addressed in New Zealand.

International approaches to transborder data flow issues

- 2.18.6 Transborder data flows were the prime reason for the involvement of the OECD in privacy issues. The approach of the OECD is illustrated by the preamble to its 1980 Guidelines which recognised that:
- although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
 - automatic processing and transborder flows of personal data create new forms of relationships amongst countries and require the development of compatible rules and practices;
 - transborder flows of personal data contribute to economic and social developments;
 - domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows.

- 2.18.7 The 1981 Council of Europe Convention No 108 also recognised in its preamble the necessity to reconcile “the fundamental values of the respect for privacy and free flow of information between people.” In 1991 the Council amplified its approach by issuing recommendations recognising that personal data should not be transferred into states which “are not in conformity” with the Convention unless necessary measures have been taken to respect principles in the Convention such as:

- contractual provisions reflecting Convention principles and with the data subject given the possibility to object, or;
- obtaining the data subject's free and informed consent in writing.¹²⁴

The recommendations also suggest that measures should be taken to avoid data

“A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these guidelines or where re-export of such data would circumvent its domestic privacy legislation.”

- OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, 1980

¹¹⁹ See, for example, “Ombudsman Order Freed Home Details”, *New Zealand Herald*, 26 June 1998.

¹²⁰ See case note no 6998. Another complaint, still under investigation, concerns a joint Australia-New Zealand agency which stores its New Zealand records in Australia and which has claimed therefore that the information is unavailable to the individual seeking access.

¹²¹ See Report of the Privacy Commissioner to the Minister of Justice on the Passports Bill, July 1992, and on the Trans-Tasman Mutual Recognition Bill, April 1997.

¹²² See GCS Information Privacy Code 1994 and EDS Information Privacy Code 1997.

¹²³ See submissions R1-R8, R12-R14, G6, G10, G13, G14, G17-G19, G21, S2, S11, S37, S42 and S45.

¹²⁴ Council of Europe, Recommendations on Communication to Third Parties of Personal Data held by Public Bodies, Recommendation R(91)10, September 1991.

being subject to automatic transborder communication without the knowledge of the individuals concerned.

- 2.18.8 A similar approach to that taken by the OECD and Council of Europe was taken in 1990 United Nations Guidelines for the Regulation of Computerised Personal Data Files. Accordingly, during the 1980s and early 1990s, the international approach to the issue of transborder data flows has been to encourage consistent privacy law in jurisdictions which may transmit, receive or process personal data, and so long as the relevant privacy laws are comparable, to thereby avoid the need to place any additional restrictions on transborder data flows.
- 2.18.9 However, the international instruments all recognise that controls may be appropriate in two exceptional cases:
- where a recipient country does not “substantially observe” the guidelines (the OECD terminology), where there are no “reciprocal safeguards” (UN) or where there is no “equivalent protection” (Council of Europe);
 - where the exported data is routed through an intermediary country with satisfactory privacy laws in an attempt to circumvent the originating country’s privacy laws: “where the re-export of such data would circumvent its domestic privacy legislation” (OECD) or “where the transfer is made ... through the intermediary of the territory of another party in order to avoid such transfers resulting in circumvention of the legislation” (Council of Europe).
- 2.18.10 Clause 17 of the OECD Guidelines provides in full:

“A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection.”

- 2.18.11 The emphasis given in the respective OECD and European instruments has meant that most European privacy laws contain express transborder data controls whereas most laws based on the OECD Guidelines (like New Zealand) do not. Section 12 of the Data Protection Act 1984 (UK) for example, implemented the Council of Europe Convention, by giving the UK Data Protection Registrar (equivalent to the Privacy Commissioner) a limited power to prevent personal data being transferred to a place outside the UK if satisfied that there is likely to be a contravention of one of the data protection principles as a consequence of the transfer.

EU Directive and transborder data flows

- 2.18.12 Interest in the matter of transborder data flows was rekindled in the 1990s through the involvement of the European Union in privacy matters. The EU’s approach has changed the relatively relaxed way that the OECD and other bodies tackled the issue. Article 25 of the EU’s 1995 Directive provides that EU countries *must* provide that the transfer of personal data to third countries for processing may take place only if the third country ensures “an adequate level of protection”. The importance of the EU in international trade has meant that this requirement has refocused attention in a number of countries on whether their laws would be adequate in European eyes and also whether their own approach to data exports is appropriate.

2.18.13 Transborder controls are being re-evaluated in EU countries which need to implement the directive in national law. Section 12 of the Data Protection Act 1984 (UK) is inadequate to meet the Directive’s requirements. Instead a new data protection principle has been proposed which states:

“Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”¹²⁵

2.18.14 Jurisdictions outside Europe are looking to the possibility of transborder data flow controls not simply to protect the data of their own citizens but also to ensure that their jurisdictions are not perceived as conduits for transfers to “data havens” for which direct transfers would be banned. Hong Kong, Quebec and Taiwan have already adopted controls.

2.18.15 The transborder data flow controls in section 33 of the Hong Kong law only take effect if the Hong Kong Ordinance ceases to apply.¹²⁶ Where the transfer of data is accompanied by a loss of control of the data, section 33 applies. This permits a transfer where it is to a jurisdiction possessing “any law which is substantially similar to, or serves the same purpose as, this Ordinance” and the Privacy Commissioner may specify such jurisdictions by Gazette notice. Also permitted are transfers justifiable on public interest grounds, or which further the interest of the individual concerned. In all other cases section 33 subjects the transferor to a duty to take all reasonable steps to ensure that the transferee applies similar data privacy standards to those applicable in Hong Kong. It is for the transferor to assess the situation and take the most appropriate steps. Consideration has to be given to such measures as obtaining contractual assurances and in this respect the Hong Kong Commissioner has released model contractual conditions.¹²⁷ The Commissioner can receive complaints relating to an alleged breach of the transferor’s duty. The Hong Kong prohibitions are enforced by an enforcement notice procedure.

2.18.16 In my view, the Privacy Act should be amended to address more precisely the circumstances in which transborder data flows should be prohibited or subjected to additional controls. In doing so it is unnecessary to adopt the restrictive EU model which has also been adopted in Hong Kong. New Zealand is a not member of the European Union and it is the OECD Guidelines to which we should primarily direct our attention. However, the EU Directive *is* relevant in so far as it is desirable to make sure that the New Zealand law, in the context of any transborder data controls, offers “adequate protection” in EU eyes. By this, I mean that any controls adopted should be able to be utilised in circumstances where it appears that a European data controller is transferring information using New Zealand as an intermediary in an attempt to circumvent European laws.

2.18.17 In this regard, I draw attention to the fact that Europeans might consider New Zealand’s law contains no effective restriction on onward transfer in such circumstances. Restrictions on onward transfers have been suggested as a “core

¹²⁵ Data Protection Bill [HL] (UK), introduction version, Schedule 1 (Part I), principle 8. The scheme is further spelt out in the second part of Schedule 1 and in Schedule 4.

¹²⁶ To relate this to a New Zealand situation, section 10 of the Privacy Act 1993 makes it clear that the privacy principles continue to apply to certain information held by New Zealand agencies overseas. If the Hong Kong approach were to be taken, any special transborder data flow controls would only apply if the New Zealand agency relinquished control in terms of section 10.

¹²⁷ Office of the Privacy Commissioner for Personal Data, Hong Kong, fact sheet no 1, “Transfer of Personal Data Outside Hong Kong: Some Common Questions”, May 1997.

principle” for assessing the existence of “adequate protection” in a particular jurisdiction.¹²⁸ One commentator has already suggested that the core principle concerning restrictions on onward transfers is a logical closing of a loophole which could otherwise be used to circumvent the restrictions on transfers from the EU by an intermediate transfer through a “safe” third country. The same commentator has suggested that the principle weakens the case for adequacy of what is otherwise one of the strongest privacy laws outside Europe, that of New Zealand.¹²⁹

Transborder data flow proposal

- 2.18.18 It should be possible to create a mechanism to control or prohibit the export of personal information in circumstances where an official body from a country having export controls compatible with the OECD approach requests New Zealand to take action in respect of a particular transfer of information utilising New Zealand as a conduit to circumvent its own privacy laws. The resultant provision might resemble “mutual assistance” provisions found in other contexts. The enforcement mechanism might be modelled upon the “transfer prohibition notices” provided for in section 12 of the Data Protection Act 1984 (UK). If this approach were to be taken there would be a number of issues to be worked through such as:
- which official requests are to be recognised - the mechanism would need to work for both European and non-European countries and be compatible with the OECD approach;
 - whether the transfer prohibition notice is to be a function exercised by the Privacy Commissioner (as it is in the UK), the government (by Order in Council, Ministerial Order, Gazette Notice etc) or on application to the courts or Tribunal;
 - the precise effect of such a notice and what steps the agency is required to take so as to resume the data exports;
 - whether there are to be appeal mechanisms and, if so, whether the Complaints Review Tribunal should be used.
- 2.18.19 If there are to be express controls on transborder data flows it would seem anomalous to give special protection to the information flowing through New Zealand from other countries and not consider the position of information about New Zealanders themselves. Again, I do not suggest that the restrictive approach of the EU Directive be adopted as I believe that principle 11 taken together with section 10 provides, for the most part, an adequate framework. However, I believe that these would be enhanced by the addition of controls which could be exercised in exceptional cases through:
- a transfer prohibition notice - of the type existing in section 12 of the Data Protection Act (UK) and suggested above as a means to counter the use of New Zealand to circumvent other countries’ data export controls; and
 - a code of practice.
- 2.18.20 I have not attempted to draft a transborder data flow provision, but have instead indicated my support of such a provision or provisions and indicated the elements I believe should be incorporated. The proposal that I have made is for a transborder data flow control at the “weaker” end of the scale. It is intended to be one step along from having no such controls at all. We live in an increasingly globalised environment and I have no wish to create excessive or unnecessary barriers to transborder data flows. As already observed the OECD Guidelines attempted to avoid such barriers although acknowledging the legitimacy

¹²⁸ See Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Reflections on Transfers of Personal Data to Third Countries - Possible ways forward in assessing adequacy, June 1997, clause 3(i)(6).

¹²⁹ Graham Greenleaf, “The European Union’s Privacy Directive - New Orientations on its implications for Australia”, Australian Privacy Summit, Sydney, October 1997.

of controls in some circumstances. However, I believe that it will be increasingly untenable to maintain a privacy law with no mechanism at all for data export controls. The emphasis I have placed in my proposal is on the creation of a mechanism for use in *exceptional* circumstances. In this respect, the proposal differs significantly from that adopted in the European Union and Hong Kong. The exceptional cases include attempts to circumvent EU controls and therefore the proposal will work in harmony with the EU Directive and rebut any suggestion that New Zealand’s law should be seen as “inadequate”.



RECOMMENDATION 35

The Act should be amended to include express provision for controlling transborder data flows, consistent with clause 17 of the OECD Guidelines and the emerging international approach to data export. In particular, consideration should be given to providing:

- (a) a mechanism which would enable mutual assistance to be extended to prohibit data exports in circumstances where New Zealand is being used as a conduit for transfers designed to circumvent controls in EU and other privacy laws;
- (b) mechanisms for imposing restrictions concerning categories of personal information for which there are particular sensitivities and in respect of which the recipient countries would provide no adequate protection.

2.19 SECTION 11 - Enforceability of principles

2.19.1 Section 11 provides that where a public sector agency holds personal information, the individual concerned has a legal right of access under principle 6 that may be enforced by court order. However, in relation to information held by private sector agencies one must work through Part VIII of the Act for enforcement of an individual’s principle 6 entitlement.

2.19.2 The intent of section 11 was to preserve existing legal rights conferred by the Official Information Act. The position was taken that a right conferred by statute should not lightly be taken away. However, it was not considered appropriate that the access entitlement in relation to private sector agencies be directly enforceable through the courts. It was recognised that a more cost effective way of enforcement is through investigation and conciliation by an independent public official who specialises in information privacy. There was generally little support in submissions for giving the ordinary courts a greater jurisdiction to consider complaints of interference with privacy.¹³⁰

2.19.3 The position is generally satisfactory in principle from my perspective. One problem in operation has been that due to the base funding of my office being outstripped by the volume of complaints I have had to queue complaints. That of itself does not provide a good reason to change the balance struck in section 11 which remains, in my view, sound. However, it does reinforce another one of the unfortunate consequences of a lengthy complaints queue which is to place some complainants in a favourable position by allowing the possibility of “jumping the queue” to seek an enforceable order through the courts.

Private prosecutions

2.19.4 Notwithstanding the existence of the right to enforce access rights to information held in the public sector through the courts, the right is rarely exercised except in one circumstance. The one circumstance involves the individuals

¹³⁰ Eleven submissions opposed extending the jurisdiction of the courts (see submissions UV3-UV5, UV8, UV10-UV13, UV16, S36 and S46). Three submissions thought that the courts should have a further role (UV1, UV6 and S42). One explained that complainants should be able to select a wider range of complaint avenues (UV1) and another thought the courts should be able to hear access or disclosure complaints after the Commissioner’s processes were complete (UV6).

“The courts, like the Ritz Hotel, may be open to all but only a few can afford the rooms. It not surprising that no individual requester of personal information has taken the matter to court.”

- EAGLES, TAGGART LIDDELL,
FREEDOM OF INFORMATION IN NEW
ZEALAND, 1992

who have been charged with an offence. Essentially principle 6 rights are the basis for the accused person to have access to personal information held on prosecution files.¹³¹ This right is enforced through the courts.

- 2.19.5 The current arrangements for having access to information in the course of criminal proceedings is not perfect. For that reason a proposal is being studied to create a specific statutory criminal disclosure regime.¹³² In the medium term there is therefore the prospect of important enhancements to the processes. However, in the meantime the Privacy Act access regime underpins the criminal discovery process. In the light of that, I have some concerns as to the limitation of legal rights in cases where a prosecution is brought by an agency which is not a “public sector agency”. Although such prosecutions concern a tiny proportion of all prosecutions brought, they are by no means unknown. For example, I understand that both the NZ Law Society and the SPCA occasionally bring prosecutions but neither are “public sector” bodies for purposes of the Privacy Act. Nor are they subject to the access regime in the Official Information Act. There has also been talk recently of the prospect of more private prosecutions being brought than has hitherto been the case.
- 2.19.6 Where private sector agencies bring prosecutions they will be subject to information privacy principle 6. The accused person is entitled to seek access to information held by such agencies so as to help prepare a defence. However, the issue is not the direct applicability of information privacy principle 6 to the agencies bringing private prosecutions but whether *the courts* can enforce those entitlements. It appears from section 11 that they cannot.
- 2.19.7 The individual could enforce the access entitlements through parallel processes involving my office and the Complaints Review Tribunal but this would not be satisfactory, particularly if court proceedings progress at a different pace from complaints processes carried out under the Privacy Act (which is quite likely with the current complaints queue).
- 2.19.8 I suggest therefore that section 11 should be amended so as to extend the entitlements which are “legal rights” beyond those presently specified in section 11(1) to include the entitlements conferred by principle 6(1) in so far as they relate to personal information held by an agency, which is not a public sector agency, where that agency has initiated criminal proceedings against the individual. I believe that the change is warranted so as to ensure that the accused person’s rights are not diminished merely by the status of the person bringing the prosecution and to ensure that the courts have the necessary powers to supervise the process.



RECOMMENDATION 36

Section 11 should be amended so that the entitlement under information privacy principle 6(1) to have access to information held by an agency is a legal right in circumstances where the agency is prosecuting the individual for an offence.

¹³¹ The resultant process, sometimes referred to as “criminal discovery” (to equate with the “discovery” process used in civil proceedings), also involves the court exercising jurisdiction in relation to the Official Information Act and common law obligations.

¹³² See Ministry of Justice and Department for Courts, Consultation paper regarding Preliminary Hearings And Criminal Disclosure, October 1997.