

Part VII

VII

Public Register Personal Information

231

“Public bodies should be able to avoid the communication to third parties of personal data which is stored in a file accessible to the public and which concern data subjects whose security and privacy are particularly threatened.”

- Council of Europe, *Recommendations on Communications to Third Parties of Personal Data held by Public Bodies*, 1991

“Drawing general principles is a challenging task. Precedents can be found from one extreme to the other. Some records are entirely public and available for use without restriction. Some records are not available to the public under any circumstances. There are a variety of intermediate models that illustrate partly open or partly confidential disclosure systems, with either statutory, regulatory, or wholly discretionary standards.”

- Robert Gellman, *Public Records: Access, Privacy, and Public Policy*, 1995.

“The newspaper industry recognises that there are significant issues of practicality and individual safety which arise from the publication and availability of public registers. Nevertheless, we firmly believe that the general rule should be that a public register is just that - public - and that inappropriate use of any register is solved in other ways.”

- Commonwealth Press Union, submission T8

“No matter what work is done to make the PRPPs adequate, they still rely to a large extent on the legislation establishing the public register.”

- Franklin District Council, submission T2

7.1 INTRODUCTION

Overview

- 7.1.1 Part VII concerns public register personal information. It includes sections 58 to 65 of the Act and links to the Second Schedule which sets out the public registers covered. After looking at some aspects of terminology, this part of the report surveys public register issues and risks and notes aspects of consultation on the issue. The report then moves to a section by section commentary and analysis with recommendations as appropriate.

Terminology

7.1.2 This part of the report is concerned with the privacy issues surrounding registers of personal information maintained by public authorities. Registers are essentially formal records set down in a systematic way for use and retrieval. The registers that this paper is particularly interested in are those to which the public has been given a right of search, such as:

- the register of land titles held at the Land Transfer Office;
- the register of motor vehicles maintained by the Land Transport Safety Authority on behalf of the Ministry of Transport.

7.1.3 Since they are usually maintained by public authorities under the authority of an enactment, registers will be referred to in this part of the report as “statutory registers”. Most of the discussion will focus upon those statutory registers for which a special right of public search is granted in the relevant enactment.

7.1.4 The Privacy Act has identified certain statutory registers which are open to search and applied special controls to them. The statutory registers maintained under the enactments listed in the Second Schedule to the Privacy Act are referred to as “public registers”. Note that “public register” therefore has a special technical meaning in the Act and does not refer to all statutory registers open to public search.

Council of Europe Recommendation R(91)10

7.1.5 Although the Council of Europe Convention No 108 generally makes no distinction between the protection of personal information in the public and private sectors, it has issued recommendations which are specific to “personal data held by public bodies”.¹ In general terms this equates to information on public registers. Parliament has directed me in section 13(1)(e) to have regard to the Council of Europe Recommendations on Communications to Third Parties of Personal Data held by Public Bodies when reviewing the public register privacy principles. I quote an extract from the preamble:

“Noting that automatic data processing has enabled public bodies to store on electronic files the data, including personal data, which they collect for the purposes of discharging their functions;

Aware of the fact that new automated techniques for the storage of such data greatly facilitate third party access to them, thus contributing to the great circulation of information within society ...

Believing however that automation of data collected and stored by public bodies makes it necessary to address its impact on personal data ... which are collected and stored by public bodies for the discharge of their functions;

Noting in particular that the automation of personal data of personal files has increased the risk of infringement of privacy since it allows greater access by telematic means to personal data ... held by public bodies as well as communication of such data ... to third parties;

Mindful in this regard of the increasing tendencies on the part of the private sector to exploit for commercial advantage the personal data ... held by public bodies as well as the emergence of policies within public bodies envisaging communication by electronic means of personal data ... to third parties on a commercial basis;

Determined therefore to promote data protection princi-

¹ Council of Europe, Recommendations on Communication to Third Parties of Personal Data held by Public Bodies, R(91)10, 1991 (hereafter referred to as Recommendation R(91)10).

ples based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data to ensure that the communication by public bodies of personal data ... to third parties, in particular by electronic means, has its basis in law and is accompanied by safeguards for the data subject;

Noting in particular that these data protection principles should be reflected in the new automated context which now characterises the communication of personal data ... to third parties under legal provisions governing accessibility by third parties to personal data ...”

I will make further reference to Recommendation R(91)10 below, especially in relation to public register privacy principles 1, 2 and 3.

Public register issues and risks

- 7.1.6 Public registers have particular characteristics which carry special privacy risks and raise difficulties in legally and practically addressing those risks in an effective fashion.
- 7.1.7 In considering the privacy risks one should bear in mind the following characteristics of a typical public register:
- the information on the register will be logically arranged to enhance analysis, use and retrieval of the data - while this is essential to the proper functioning of the register for its necessary purposes, it also makes it an especially attractive source of information for other purposes;
 - only key authoritative data is registered - unlike many other structural record systems (such as government files) a statutory register is unlikely to be cluttered with extraneous material such as draft documents or correspondence, making it straightforward to quickly locate relevant information;
 - the existence of the register will be well known - making an easier source for third parties searching for data;
 - the register will have a degree of institutional permanence - which may enable third parties to plan elaborate and ongoing processing of the data for unrelated purposes;
 - individuals will be compelled by law to supply personal information for the register or else they will commit an offence or be unable to undertake some activity - this compounds the affront to privacy when information is used for unrelated purposes;
 - certain sets of information exist only in public registers since individuals are unwilling to provide the information voluntarily;
 - a statutory right to search the register exists which restricts a registrar’s discretion to withhold information.
- 7.1.8 Accordingly, many public registers are attractive propositions for all sorts of third parties who would wish to use them to obtain information about individuals - indeed, some businesses specifically “mine” public registers and sell the results. Briefly stated, the central privacy issues with public registers revolve around the fact that individuals have no choice but to supply their public details which may then be published and will be given out on request to whoever wishes to have the information without regard to the purpose for which that information will be used or the harm that any such use may cause an individual.
- 7.1.9 Typical public register privacy problems are:
- their use for tracing individuals for reasons unconnected with the purpose for which the register was established, whether those reasons be relatively benign (preparing a family history) or malign (tracking an estranged partner who has fled from an abusive relationship);

“Council does receive complaints from time-to-time from members of the public regarding the use of public register information by direct marketing companies and the like.”

- TAURANGA DISTRICT COUNCIL,
SUBMISSION T7

- bulk retrieval of personal information on public registers by commercial interests which use and sell the information for direct marketing purposes or for profiling individuals (for instance, as to their wealth or creditworthiness).

- 7.1.10 The nature of public registers also creates difficulties in tackling the privacy problems effectively. Some of these difficulties include:
- the fact that many statutory provisions give little explicit guidance as to the purpose for which a register was established;
 - few statutory provisions establishing registers themselves attempt to address any privacy issues;²
 - the evolution from traditional paper-based, and office-bound, registration systems to automated systems, with potential for on-line searching, removes previous privacy protection which incidentally existed through physical constraints and inefficiencies and the need for human intervention;
 - the interaction between two pieces of legislation, the Privacy Act and the public register privacy provision;³
 - the compulsory, or non-voluntary nature of the registers, restricting the use of authorisations, or opt-in/opt-out provisions which are often a suitable mechanism for resolving privacy problems in other contexts;⁴
 - the lack of data protection “infrastructure”, such as audit mechanisms, rules out some otherwise feasible privacy solutions.

Consultation

- 7.1.11 Since 1993 significant thought has been given to public register privacy issues. I have, for example, encouraged discussion of the issue at the annual Privacy Issues Forum. Papers prepared for these conferences included in 1994, 1995 and 1997:
- Public registers - A discussion paper;
 - Public register privacy issues - some issues for local government;
 - Public registers and profiling;
 - Public registers and personal safety;
 - Public registers - recent developments and what’s wrong with the public register privacy principles.

- 7.1.12 To further inform discussion about public register issues, and promote compliance with the public register privacy principles, my office released in 1997 a compilation of materials on the subject.⁵ From my 1995/96 annual report onwards I have reported on public register issues in a separate part of my annual report. I have also been active in scrutinising, and reporting to you in relation to, proposed legislation bearing upon the statutory registers open to public search.

² Sometimes bodies maintaining statutory registers make decisions to protect privacy within the bounds of their statutory powers. For example, a registrar might choose not to place residential addresses on a public register notwithstanding that the statute is silent on the matter. However, what I am noting here is that very few statutory provisions themselves seek to address privacy issues. The few that do usually permit an individual to apply to have their details treated in a special way. Such provisions usually turn upon some objective grounds rather than a desire for privacy. For example, an elector is permitted to have details withheld for personal safety from the published electoral roll. Under the Building Act 1991, plans to be placed on a building consent register can be marked “confidential” by owners for reasons of security or copyright.

³ With the Domestic Violence Act 1995 as a further player and, on occasion, the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, making a showing.

⁴ However, the Radiocommunications Amendment Bill, presently before Parliament, attempts in an innovative way to address the matter through the inclusion of an “opt-in” arrangement whereby address details will not be released except with the authorisation of the individual (since in that instance the disclosure of address details is not required for any official or necessary purpose of the register but registered individuals may find it personally beneficial to have their details released to associations of radiotransmitters). See Report of the Privacy Commissioner to the Minister of Justice in relation to the Radiocommunications Amendment Bill, 19 January 1998.

⁵ A Compilation of New Zealand Materials in Relation to Public Register Privacy Issues, January 1997.

- 7.1.13 As part of the consultation on this review I released a 28-page discussion paper in September 1997. Thirty-one submissions were received. A consultation meeting held with representatives from a variety of Wellington region local authorities was held in Wellington in December 1997. Although the meeting canvassed other local authority issues the main focus of discussion was public register issues.

SECTION BY SECTION DISCUSSION

7.2 SECTION 58 - Interpretation

- 7.2.1 Section 58 defines three terms specifically for Part VII. None of the definitions has given difficulty in operation. Issues I will canvass are:
- whether it would make the Act more “user friendly” if the definitions were located in the general interpretation provision, section 2;
 - whether there is a case to extend the meaning of “public register” to include all statutory registers open to search; and
 - whether there is a case for further definitions.

Location of definitions

- 7.2.2 Section 58 defines three terms: public register, public register privacy principle and public register provision. Each of these is principally, but not exclusively, to be found in Part VII. For example, “public register” is also to be found within the definition of “publicly available publication” which is used in Parts I and II. “Public register privacy principle” is found also in both Parts II and VIII.

- 7.2.3 Both “public register” and “public register privacy principle” are defined in section 2. In each case, the relevant definitions simply say that the term “has the meaning given to it in section 58”. I do not believe that the operation of the Act would be enhanced by moving the section 58 definitions into section 2.

Definition of “public register”

- 7.2.4 The term “public register” is currently defined to mean:
- (a) any register, roll, list, or other document maintained pursuant to a public register provision; or
 - (b) a document specified in Part II of the Second Schedule.
- The list of public register provisions is set out in the Second Schedule to the Act and Appendix I of this report.

- 7.2.5 Accordingly, a statutory register open to public search will only become a “public register” in terms of the definition when it has been suitably identified in the Second Schedule. It follows that there may well be a number of registers, rolls, lists or other documents maintained pursuant to enactments which have similar characteristics to the existing “public registers”. Indeed, that is clearly the case.⁶ Although the list in the Second Schedule captures many of the more important registers it is by no means comprehensive. Aspects of this issue have already been canvassed in the preceding introductory section of this part of the report and I will return to it in relation to section 65.⁷

- 7.2.6 A suggestion, made in several submissions, is that “public register” be redefined to include all statutory registers open to public search rather than just those listed in the schedule.

- 7.2.7 A suitable definition might be:

⁶ Discussion paper No. 5 listed some 50 statutes understood to contain provisions establishing statutory registers which are not “public registers”.

⁷ See paragraph 7.14.

Public register means any register, roll, list or similar document:

- (a) maintained pursuant to a provision contained in an enactment; and
- (b) which is required to be open to public search pursuant to a provision in that enactment.

- 7.2.8 The elements of such a definition indicate:
- that the register must have a register-like form - that is, being a register, roll, list or other similar document;
 - that it be maintained pursuant to a provision in an enactment - that is having a “public” and official character being maintained under law;
 - be open to search - that is having a “public” character in the sense of the information on the register being accessible to the public;
 - that it be a legal right of access - that is, that the register be required to be open to search by law rather than for its openness to be a matter of administrative discretion and to distinguish a register from the more general availability of official information under the Official Information Act.⁸
- 7.2.9 If such a definition were to be adopted it would be possible to dispense with the Second Schedule and the specific listing of public registers. It would be possible to modify the definition so that a “public register” includes those maintained pursuant to a public register provision set out in the schedule *and* any other register of the type coming within the general definition.
- 7.2.10 In my view, it would be possible for the regime to work suitably in relation to a general definition to be drafted. The fact that the public register controls defer to other enactments will mean that significant operational problems would be unlikely to be encountered.
- 7.2.11 However, I recommend continuing with the present definition and to couple this with a systematic effort to identify registers having the characteristics of “public registers” and add them to the Second Schedule. It seems to me that the making of a conscious decision to add an entry to the list of public register provisions is a valuable one. It retains certain advantages over the adoption of a general definition, including:
- the effect of the extension of public register controls to a wider range of registers will be better understood;
 - certainty with respect to the scope of any extension of the regime;
 - the resultant schedule will provide a picture of the series of registers to which the regime applies and this transparency or openness is a desirable objective of data protection laws;
 - the effect of disclosure under principle 11 will be clearer;
 - the agencies which administer the registers will better understand their responsibilities if they have participated in identifying the relevant provisions and have been consulted on the application of the regime to them;

⁸ Obtaining information from a register pursuant to a statutory search right differs in nature from an Official Information Act request. In an Official Information Act request, the requester sets the parameters through the scope of the request. A register search, on the other hand, does not usually have this individualised quality. Requests for information from a register must fit the requirements of the agency maintaining the register and not the other way round. A request under the Official Information Act requires an official to consider whether there are grounds for withholding the information. Judgment and discretion are called for, and occasionally consultation. The official may withhold information although before doing so will consider any countervailing public interest favouring disclosure. A request for information from a public register is far more mechanistic. If the registrar’s requirements are met, such as through the use of a search form or the payment of a fee, the information in standardised form will be released, usually quite promptly. The Official Information Act does not derogate from provisions in enactments which authorise or require official information to be made available. Statutory search rights concerning registers are such provisions.

- there seems to be little privacy “downside” in the delay inherent in systematically bringing further registers into the regime - the information on the registers remains subject to the information privacy principles;
- the opportunity for Parliament to define the purposes of a register as it takes the decision to add a provision to the schedule.

Possible new definitions

7.2.12 In the discussion paper on this Part of the Act I sought views upon whether certain terms used in Part VII should be defined. I also asked whether any other terms should be defined. Amongst the terms considered were “re-sorted” and “combined”, used in public register privacy principle 2, and “electronic transmission” and “member of the public”, used in principle 3. At this point I simply observe that in my view it is not necessary to provide further statutory definitions at this time.

7.3 SECTION 59 - Public register privacy principles

7.3.1 Section 59 establishes the four public register privacy principles. They cover the following topics:

- principle 1 - search references;
- principle 2 - use of information from public registers;
- principle 3 - electronic transmission of personal information from registers;
- principle 4 - charging for access to public register.

There follows a discussion of each principle with suggestions for two further principles.

7.4 PRINCIPLE 1 - Search references

7.4.1 Public register privacy principle 1 states:

PRINCIPLE 1

Search references

Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised.

7.4.2 The term “search reference” is not defined but the meaning seems clear. It refers to the information that must be cited by the public when seeking to obtain information from a register. Typical search references include:

- name;
- address;
- licence or document number.

7.4.3 Search references have traditionally relied upon the way in which a register is organised. For example, if certificates of naturalisation are stored in filing cabinets in date order depending upon the day on which citizenship is granted it is likely that the search references would be sequential document number, date of citizenship, or for a broader search, year of citizenship. Retrieval based on a person’s name would not be possible.⁹ Conversely, if the register was organised alphabetically by surname of new citizen it would not be possible to search solely by document number or date of citizenship. To compensate for the physical limits on easy retrieval of data, registrars would typically prepare an index to enable ready retrieval by other appropriate search references.

7.4.4 The principle makes it clear that the agency maintaining the register can only allow the information to be made available by search references which meet the principle’s criteria. Looked at from the other side of the counter, a person

⁹ Although typically an *index* by name would also be prepared to allow for such retrieval.

searching the register could not insist on having access to information by citing some other reference (in the example given, by citing country of origin).

Search references and purpose of a register

7.4.5 When legislation establishes a new register, officials have the task of devising suitable administrative arrangements. At the point of establishing the register officials are keenly aware of the purpose for which it has been established and fully understand the need for the relevant information to be retrievable for the appropriate purposes. For example, in establishing a register of motor vehicles it will be known that the information will need to be retrieved by licence plate number whereas there may be little need to retrieve information by reference to other information held, such as vehicle colour. If there is no legitimate need to search such a register by individual's name it is unlikely that the search reference will be built in to the way that register is indexed or organised.

7.4.6 The brevity and simplicity of the principle belies its importance. Search reference limits often act as an effective privacy protection device. By prohibiting the addition of search references inconsistent with the manner in which the register is indexed or organised there is thereby a privacy protection. For example, a search by owner's name using the vehicle register would effectively create a national locator of persons, something that would not have been the subject of debate in creating the register.

7.4.7 Notwithstanding the preceding discussion, it does not always follow that existing search references will mirror the purposes for which a public register has been established and public search rights granted. Reference to "the manner in which the register is indexed or organised" is an imperfect way of seeking to ensure that the search references enable access to the personal information held consistently with the purpose for which the register was established. Strictly speaking the most the principle would achieve is that the registrar "calls the shots" in that the member of the public cannot insist on search references which differ from those inherent in the register's organisation or contained in the agency's index. Although, as suggested, the existing principle should ensure some correlation with the purposes underlying the register, this is not explicit and will not be borne out in some cases (for example, if a very broad index, with many search categories, had been created).

7.4.8 Furthermore, the computerisation of such records, together with advances in the flexibility of computer database programs, means that items of information can be accessed and sorted in countless ways without obvious effort. In such computer systems some would argue that it is perhaps no longer meaningful to think of the register being "indexed or organised" by some limited set of search references. For those systems - and *a fortiori* for the next generation of database technology - the existing principle 1 may be simply ineffective.

7.4.9 I examined the possibility of incorporating within the principle an express reference to a register's "purpose". In the relevant discussion paper I proposed that the principle be amended to read:

Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised *and with the purpose of the register.* [change highlighted]

7.4.10 Most submissions supported the proposed change seeing it is as an appropriate way to tackle the privacy issues.¹⁰ Particularly notable was the strong support

¹⁰ Sixteen out of 18 submissions agreed that principle 1 should require search references to be consistent with the purpose of a register - see submissions T1, T9, T11-T15, S27, S36, S42, S51 and S58. One submission opposed the proposition (T10) while submission T17 considered that this was already required under the current principle.

“You may be aware of this Council’s prolonged challenge regarding the ability of organisations to access personal information from the building consent register. The outcome favoured releasing the information. It is frustrating, therefore, that such an outcome would seem to totally contravene the spirit of the Privacy Act. Irrespective of the prevailing legislation, this Council firmly believed that more weight should have been given to the purpose of the collection of the information and its commercial value. Suffice to say, that along with probably every other local authority in New Zealand we are now selling on a cost recovery basis, building consent information to organisations which intrude upon the privacy of individuals to use it for commercial gain.”

shown in local government submissions. The limited opposition in the submissions came not from the agencies which maintain public registers (although some practical issues were raised in the submissions, particularly over the process for “fixing” purpose) nor from agencies representing or having a role in relation to persons whose personal information is displayed on public registers. The main submission in opposition was by a credit reporting agency (submission T10).

- 7.4.11 I have concluded that the proposed change to principle 1 would be a desirable amendment to enhance privacy and the appropriate functioning of the public register privacy principles. A reference to purpose will make the principle more understandable to anyone familiar with notions of information privacy and will directly address shortcomings in the present principle. The resultant principle will, in my opinion, be workable.



RECOMMENDATION 84

Public register privacy principle 1 should be amended so that search references be required to be consistent with the purpose of a particular register.

Establishing purpose of a register

- 7.4.12 Given my recommendation that search references be consistent with purpose, it is necessary to consider how “purpose” is to be ascertained. I have already noted that public register provisions frequently give little explicit guidance as to the purpose for which a register was established. For that reason, I canvassed in the discussion paper whether it would be desirable to establish a particular mechanism for defining a register’s purpose. If a mechanism were to be crafted there would be several issues to address:
- who would be the decision maker in fixing purpose? Candidates would include the relevant department, Minister, the Executive Council (through regulations), Parliament (through statutes) or the Privacy Commissioner (through code of practice or a new mechanism).
 - What process would be followed? For instance, would the Privacy Commissioner or public have to be consulted? Would the resultant statement be published in the Gazette?
 - What legal status would a statement of purpose have in the event of a complaint? If the purpose was established under an enactment, such as within a public register provision or in statutory regulations, this would prevail by reason of sections 7 and 60 of the Privacy Act. Similarly, if the Commissioner established statements of purpose pursuant to a code of practice, the Act would give them an automatic status.

- 7.4.13 On the subject of “purpose”, clause 4.1 of Recommendation R(91)10 states:

“The purposes for which the data will be collected and processed in files accessible to third parties as well as the public interest justifying their being made accessible should be indicated in accordance with domestic law and practice.”

- 7.4.14 For several years my office has suggested to departments which enact or re-enact public register provisions that they include a statement of any register’s purpose. As a result, for example:
- Local Government Act 1974, section 122ZI, provides that the register of charges established under that section is “for the purposes of enabling any member of the public to establish, verify, or assess the charges registered against the asset or assets of a local authority and the nature and terms of the obligations that those charges secure”;
 - Radiocommunications Amendment Bill, clauses 3 and 11, specifies that the registrar must maintain a register “for the purposes of maintaining records of interests or uses relating to radio frequencies” and that any person may

“The many statutes that require, permit, or prohibit the disclosure of specific categories of public records would appear to offer a wealth of material from which more general principles can be deduced and policies can be isolated. In practice, this is much more difficult than it appears. For many statutes, it is not possible to find materials explaining [why] the law was written in a particular way. Even if materials may be found, they may not reflect current controversies.”

- ROBERT GELLMAN, *PUBLIC RECORDS: ACCESS, PRIVACY, AND PUBLIC POLICY*, 1995

have access “for the purpose of determining whether or not any radio frequency is subject to a record of management rights, a spectrum licence, or a radio licence, and determining the identity of the owner of a management right, a right holder, or the holder of a radio licence.”

- 7.4.15 Statutory statements of purpose remain rare. Whether or not public register privacy principle 1 is amended, I believe that it continues to be desirable for new statutory registers to have that purpose explicitly stated. Statutory statements of purpose will guide the agencies administering the register as well as the users of registers and the Privacy Commissioner in investigating complaints. Any *statutory* statement of purpose will have priority in any scheme devised since it will take precedence over regulations, codes of practice or administrative decisions.
- 7.4.16 Given that few statutes currently contain statements of purpose, it is necessary to consider whether:
- all public register provisions should be amended to contain a statement of purpose;
 - an alternative mechanism for fixing statements of purpose is desirable; or
 - an amended principle 1 can operate satisfactorily without any new mechanism to fix purpose being created.
- 7.4.17 I have concluded that it would not be desirable to seek to amend, in one hit, every public register provision so as to include a statement of purpose. This would require a commitment of resources by departments and my office which is not warranted as a priority. Rather, I am content with pursuing the merits of that approach on a register by register basis as opportunities arise for review, amendment or consolidation.



RECOMMENDATION 85

As new public register provisions are enacted, or existing ones reviewed or consolidated or amended, consideration should be given to including statutory statements of purpose.

- 7.4.18 It is possible to devise a new mechanism, to be located within Part VII of the Privacy Act allowing for a statement of purpose to be fixed. Such mechanisms could include the following options:
- a power enabling regulations to be made in respect of any public register provision stating the purposes for which a public register is established and made available for public search;¹¹
 - a mechanism for the Minister or agency which maintains a public register to produce a draft statement of purposes, to notify this, undertake public consultation, and then issue a final statement by Gazette notice which has effect until revised following a similar process;
 - a Privacy Commissioner-initiated process involving the release of a proposed statement, public consultation, and issue which would be subject to Parliamentary disallowance, modelled upon, or forming part of, code of practice provisions;
 - a statutory requirement for departments to produce and have available for the public on request a statement of purposes.
- 7.4.19 Any of these alternatives is, in my view, workable. The merit in any one depends upon whether one believes such decisions should be taken at the Parliamentary, Governmental, or administrative level or by an independent Commissioner. There are also considerations of competing calls for resources, such as in relation to Parliamentary time.

¹¹ A single set of regulations is likely to be impractical. It is anticipated that regulations would be developed only as needed and perhaps included within any general sets of regulations concerning a register.

7.4.20 My view is that where a bill is before the House these decisions should be taken by Parliament. However, I do not characterise the issue as one that ought to demand Parliamentary attention in the absence of new, amending, or consolidating, legislation coming before the House. I believe that the devising of suitable statements of purposes are well within the capabilities of departments. As the stewards of the information, and as the people most familiar with their own legislation, departments should have initial responsibility for preparing any statements of purpose. Any process followed should involve proper consultation outside the department.

7.4.21 However, as a supplement to any administrative process initiated by departments, it may be useful to allow for the issue of regulations to specify purposes. Such regulations should be made after consultation with the Privacy Commissioner. It would be unnecessary to issue such regulations in respect of all public registers. However, the option would be there in the event that it is desired to obtain greater transparency in respect of a particular register. Regulations would provide an alternative to seeking a code of practice from the Privacy Commissioner and a “fast-track” alternative to obtaining amendment legislation. Accordingly, consideration could be given to placing a general regulation-making power in the Privacy Act.



RECOMMENDATION 86

Consideration should be given to establishing in the Act a regulation-making power to specify, in respect of any particular public register, the purposes for which the register is established and is open to search by the public.

7.4.22 The position for registers not having a statement of purpose in statute, regulation or code will be similar to that of practically all agencies in relation to their holding of any personal information. New Zealand does not operate a register of all permitted uses or purposes as do European countries. Judgments have to be made all the time as to what is a “purpose connected with a function or activity of an agency” or is a purpose for which information is collected or obtained (information privacy principles 2, 3, 9, 10 and 11). Even in the absence of a complaint, agencies must be ready to tell individuals the relevant purposes or to answer my queries under section 22 if necessary.

7.4.23 Formal public register complaints are not common at present and I have no particular reason, absent controversial decisions by departments to extend search references beyond the reasonable bounds of their statutory mandate, to think that this will change significantly in the future. If a complaint is received I will, as with other complaints, receive representations from the agency and complainant and will, if necessary, form an opinion as to the relevant issues. In the event of disagreement with the department I will, on the present complaints processes, provide a recommendation to the relevant department or Minister.¹²

7.5 PRINCIPLE 2 - Use of information from register

7.5.1 Public register privacy principle 2 states:

PRINCIPLE 2

Use of information from public registers

Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

¹² Privacy Act, section 61. Elsewhere I recommend that public register complaints be fully enforceable and be able to be taken to the Tribunal (see paragraph 7.10.5 and recommendation 95). In such an event it will be possible for a ruling of the Tribunal to be obtained.

“The Council agrees that public registers (not merely those restricted to local authorities) are often used for reasons unconnected to the purpose for which the registers were established.”

- PALMERSTON NORTH CITY
COUNCIL, SUBMISSION T4

Council of Europe Recommendation R(91)10

7.5.2 Clause 7 of Recommendation R(91)10 states:

“Unless permitted by domestic law providing appropriate safeguards, the inter-connection - in particular by means of connecting, merging or downloading - of personal data files consisting of personal data originating from files accessible to third parties with a view to producing new files, as well as the matching or interconnection of files of personal data held by third parties with one or more files held by public bodies so as to enrich the existing files or data, should be prohibited.”

Application to every person

7.5.3 While all four of the principles apply to agencies responsible for administering a public register, principle 2 also applies to every other person.¹³ The principle does not simply guide the actions of registrars - it also constrains the use of information obtained from public registers by other persons. The principle attempts to address the risks of information which is supplied compulsorily for public registers being reprocessed for other purposes without the approval of the individuals concerned. However, unlike the Council of Europe Recommendation R(91)10, principle 2 only prohibits such activities if they are carried out for the purpose of on-selling the enriched information.

7.5.4 The principle is also necessary so as to ensure that the other principles are not undermined. For example, consider a register which does not utilise the name of the individual as a search reference. Principle 1 would be undermined if a company can obtain all the information from the register and makes it available electronically through different search references. It is the same information that was obtained compulsorily and the same privacy risks arise.

7.5.5 In recommendation 95 I propose that the public register privacy principles become enforceable in a similar manner to the information privacy principles. This would enable complaints against the agencies maintaining public registers to be taken right through to the Tribunal if necessary. The proposal is also that complaints against any other agency which breached principle 2 be able to be taken to the Tribunal. I will not further repeat those recommendations here.

Layout

7.5.6 While I do not recommend any substantive amendments to principle 2 at this stage I do consider that it would benefit from a slight drafting change.

7.5.7 The principle has several elements within it which are expressed either as alternatives or as cumulative requirements. Although these elements are relatively straightforward if one takes care to consider the principle, the task is not made as easy as it might be through its layout as a single lengthy sentence. I suggest that the elements expressed as alternatives near the start of the principle be separately stated as itemised paragraphs. Accordingly, the reformed principle would read as follows:

Use of information from public registers

Personal information obtained from a public register must not be:

(c) re-sorted; or

(d) combined with personal information from any other public register:

for the purpose of making available for valuable considera-

¹³ Refer section 60(2). See also my proposal to amend that section in recommendation 94.

tion personal information assembled in a form in which that personal information could not be obtained directly from the register.



RECOMMENDATION 87

Public register privacy principle 2 should be re-enacted with a structure which more clearly leads users to identify its elements.

7.6 PRINCIPLE 3 - Electronic transmission of personal information from public register

7.6.1 Public register privacy principle 3 states:

PRINCIPLE 3

Electronic transmission of personal information from public register

Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.

Manual to computerised registers

7.6.2 This principle tackles the means by which information is increasingly made available from public registers. Traditionally registers were paper based and often consisted of files in filing cabinets or entries written in a book. Getting access to a register meant one had to visit the public office, ask to see the entry, and to have this brought to the desk for perusal. Later, with the advent of photocopiers, it became usual administrative practice, sometimes reflected in statutes, for access to be given by photocopying an extract from the register. Extracts could be made at the public office, or requested in writing, usually on payment of a copying fee. With the advent of computers, entries could be given by computer printout.

7.6.3 Until quite recently, few public registers have been completely computerised. This is becoming more usual now.¹⁴ Computerisation of the registers is becoming increasingly sophisticated. Information can be supplied on computer disk for entry on some registers. Searches on some registers can already be made on-line.

7.6.4 The principle attempts to place a brake upon making information available from public registers generally by means of electronic transmission. “Electronic transmission” encompasses, amongst other things, downloading information to disk or tape for reading by another computer as well as on-line transmission. The exceptions where electronic transmission is permitted include:

- where the purpose of the transmission is to make the information available to a member of the public who wishes to search the register - principle 3 itself;
- where a statute authorises the action - section 60(3); or
- where a code of practice authorises the action - section 64(a).

Privacy risks of electronic transmission

7.6.5 There are a variety of privacy risks associated with electronic public registers since information can be extracted and used or manipulated with ease compared with non-electronic data. For example, in electronic form:

- thousands of records can be matched against others within fractions of a second;

¹⁴ Although sometimes a “computerised” register simply mirrors paper records which comprise the legally authoritative version for certain official purposes.

- data can be added to other records with ease creating new databanks and enabling the profiling of individuals;
- sophisticated and unexpected searches can be made with ease (for example, a search of “red BMW cars owned by women living in Seatoun” is feasible electronically but not with manual records);
- errors in records can be rapidly transmitted to other databases and the effects on individuals multiplied;
- registers may be vulnerable to remote access (“hacking”) with attendant risks of disclosure, loss or alteration of data;
- electronic transmission of data may enable persons to construct a full copy or substantial extract from a public register which could then be re-worked so as to be put to different private uses.

7.6.6 This is just a selection of risks. It is not comprehensive. Nor should it be taken as an argument against computerising public registers. Good public administration precludes any suggestion that public registers be “off limits” and maintained with yesterday’s technology. However, given the nature of public registers, including the compulsion by which information is obtained and the right to public search, the implications of moving from manual to computerised processing should not be overlooked. The point at which the register interfaces with the outside world (the point of transmission or search) is a key aspect of controlling the risk.

7.6.7 The extracts from the preamble to the Council of Europe recommendations, quoted at paragraph 7.1.5, give a “flavour” of the international concern about electronic transmission of information from registers. While the Privacy Act generally takes a “technology neutral” view of the processing of information Recommendation R(91)10 supports the case for special controls relating to the electronic transmission of personal information.

7.6.8 Principle 3 can be criticised for not going as far as the Council of Europe Recommendations. For example, clause 5.2 of the Recommendations says:

“At the time of automatic communication, technical means designed to limit the scope of electronic interrogations or searches should be introduced with a view to preventing unauthorised downloading or consultation of personal data or files containing such data.”¹⁵

7.6.9 Indeed principle 3 might be seen in some respects as permissive rather than restrictive. Some agencies maintaining statutory registers seem to take an “all or nothing” approach and suggest that once the information is made available electronically it is no longer feasible for the agency maintaining the register to attempt to protect privacy interests or to control the purpose for which people using the register are searching it. This is typically the response of agencies which, perhaps without much study of the implications from a privacy perspective, make records directly available on the Internet. Sometimes such records are placed with minimal controls or controls which are easily circumvented for commercial or other purposes. I believe that there is technology available which can automatically search holdings of information on the Internet thereby enabling a vast amount of data to be downloaded to create a duplicate database searchable by whatever references the new possessor of the data chooses.¹⁶

7.6.10 Paragraph 5.2 of the Council of Europe Recommendation R(91)10 suggests that agencies should continue to recognise their responsibilities when design-

¹⁵ However, information privacy principle 5 does envisage security safeguards being taken.

¹⁶ Some of the risks have recently been canvassed in the Common Position of the International Working Group on Data Protection in Telecommunications, “Data Protection and Search Engines on the Internet”, 15 April 1998.

ing facilities to make information available electronically. For example, attention should be paid to the technical means which may be available to continue to protect the data. Where these are clearly inadequate, it is questionable whether the information should be made available electronically at all. This is especially the case with information that has been obtained compulsorily from individuals. The approach of Recommendation R(91)10 is that such information should not be made available to third parties without individual authorisation.¹⁷ Where the storage of the personal information in a file accessible to third parties is not obligatory, clause 6.2 of Recommendation R(91)10 recommends that the individual be made aware of the proposed accessibility of the information and advised of the right to have the personal information stored in a way that is inaccessible to third parties.

7.6.11 In terms of the electronic transmission of personal data held by public bodies, the Recommendation R(91)10 also states:

“Measures should be taken to avoid personal data or files containing fixed data from being subjected to automatic transborder communication to third parties without the knowledge of the data subject.” (Clause 8.4)

7.6.12 At present our Privacy Act has no such protection. I make general recommendations in relation to transborder flows of personal data and will not repeat that material here. However, while noting that principle 3 contains a general prohibition on electronic transmission of personal information from public registers, there are three exceptions.¹⁸ I would be concerned if there were to be a great rush to place New Zealand public registers containing personal information on the Internet which would make personal information generally available in jurisdictions which have no privacy or data protection laws. Were that to happen, particularly if the ability to search was free of charge, I would have little doubt that databases on New Zealanders would be created in other jurisdictions. At the very least this would create the conditions for unwanted transborder direct marketing to New Zealanders. Certainly it would create the prospect of use of the information for purposes that were never intended when the information was obtained.

7.6.13 I recommend that further study be made of the issues and the means by which the law may be amended to better address the risks. One way in which the issue might be tackled would be for the reference to “member of the public” in the principle to be amended to refer to a “member of the public *in New Zealand*”. I expect that “member of the public” is probably normally understood to mean people in New Zealand in any case. One practical effect would be that personal information contained in public registers could not be made available for search on the Internet unless:

- there was a mechanism established for limiting searches to people in New Zealand; or
- principle 3 is modified by code of practice - in which I would consider relevant privacy issues such as the sensitivity of the data, the explanations that had been given to individuals at the time of collection, and the degree of compulsion used in obtaining the information;
- the electronic disclosure to overseas enquirers is authorised by an enactment.



RECOMMENDATION 88

Public register privacy principle 3 should be amended by adding “in New Zealand” after the words “a member of the public”.

¹⁷ Clause 6.1.

¹⁸ See sections 60(3) and 64(a) and paragraph 7.6.4.

- 7.6.14 In my view a restriction of this sort is justified to inhibit any rush to place public registers containing personal information on the Internet. It may be that satisfactory technical means can be developed to limit searches to all, or sensitive parts of, databases proposed to be placed on the Internet. If that is the case, electronic transmission will be permissible in conformity with the amended principle. In other cases, it will be open to the relevant department to seek statutory authority to place a public register on the Internet notwithstanding principle 3. Again, I see that as appropriate since Parliament is often a final arbiter between personal rights and public interests. Similarly, a department can promote the idea of a code of practice. Were a department to do so it ought to carry out a privacy impact assessment to show, amongst other things, how it is intended to:
- protect sensitive data;
 - inform individuals whose information is to be made available as to the practice; and
 - use technical means to limit the scope of electronic interrogations or searches with a view to preventing unauthorised downloading or consultation of personal information.

- 7.6.15 The recommendation that I have made is consistent with Recommendation R(91)10 to which Parliament has formally directed my attention. However, I anticipate that voices will be raised claiming that somehow the proposal unacceptably stifles innovation or new delivery of public services. Critics may argue that obtaining an amending Act of Parliament is too high a hurdle. Accordingly I propose that regulations be able to be issued under the Privacy Act to permit electronic transmission notwithstanding the proposed controls. Such regulations will take precedence over principle 3.¹⁹ The regulation making power should be exercisable only after consultation with the Privacy Commissioner.



RECOMMENDATION 89

If recommendation 88 is adopted, there should be a power in the Act to make regulations, after consultation with the Privacy Commissioner, in respect of any public register to authorise and control the electronic transmission of personal data which is not limited to members of the public within New Zealand.

7.7 PRINCIPLE 4 - Charging for access to public register

- 7.7.1 Public register privacy principle 4 states:

PRINCIPLE 4

Charging for access to public register

Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.

- 7.7.2 Rights of access to personal information granted to individuals can be undermined if significant barriers are placed in the way through fees and charges. This is recognised in the procedural and complaints provisions attached to the information privacy principle 6 right of access²⁰ as well as by this principle.

Third party charging

- 7.7.3 However, this principle goes further than addressing just the matter of the individual concerned having access to personal information held on a register. It

¹⁹ See section 60.

²⁰ Generally speaking a public sector agency cannot make a charge for giving an individual access under information privacy principle 6. A private sector agency may only make a “reasonable charge”. Complaints concerning the reasonableness of a charge can be taken to the Privacy Commissioner for determination: see sections 35, 36 and 78.

also applies to third parties, such as direct marketers, seeking access to personal information held on a public register. In those circumstances a different set of issues arises. Keeping charges to third parties low or to a “reasonable” level does not necessarily protect or enhance privacy. Indeed, in some circumstances that could work against privacy interests if it means that commercial interests can, for no charge or for a very modest fee, obtain information which has been collected compulsorily which they could not obtain if they had to meet the costs of collection themselves.

- 7.7.4 I have concluded that principle 4 goes further than is necessary to protect privacy interests and by doing so it has the potential to place the Commissioner in the position of adjudicating on complaints about excessive charging for access to information the use of which is likely to be detrimental to an individual’s privacy. My qualms about exercising such a function arise because there is the potential for conflict with my privacy role. For this reason I consider that principle 4 should be amended to read as follows:

Personal information on a public register shall be made available *to the individual concerned* for no charge or for no more than a reasonable charge [change highlighted].



RECOMMENDATION 90

Public register privacy principle 4 should be amended so that the constraints upon charging for access to personal information from a public register apply only in relation to the making available of information to the individual concerned.

- 7.7.5 The agencies maintaining public registers could ensure compliance with the amended principle in a variety of ways. They could:
- make no charge for access to the register at all;
 - make no charge for access to the register by the individual concerned but levy a charge for a search by any other person;
 - levy a common charge for access by the individual concerned or any other person, set at a level that is “reasonable” in respect of the individual concerned;
 - make a lower charge for searches by the individual concerned than for others;
 - establish the charging regime by regulation - which would override the principle pursuant to section 60(3).
- 7.7.6 The proposal for partial “deregulation” would *not* require registrars to maintain a separate charging regime for requests by individuals if they did not wish to do so. It would be open to them to levy a higher charge for access by anyone other than the individual concerned.²¹ However, as now, registrars can simply keep all search fees to a reasonable level. In fact, I expect that charges in respect of a number of registers are set by regulations in any case. It would be open for individuals to complain to me under section 61(1) if regulations set charges which were excessively high.
- 7.7.7 I am suggesting that principle 4 not be the legal determinant of such matters. If public authorities wish to raise the costs to third parties of searches of public registers then this is, to my mind, a matter which can be satisfactorily determined outside the framework of the Privacy Act.
- 7.7.8 In respect of central government agencies, the approach to pricing presently recommended by Cabinet is contained in the State Services Commission *Policy*

“As it stands, this principle means that commercial entities are able to get information at far less than its market value and thereby make a profit, which is at the expense of the public in the end. Thus it is understandable that some local authorities should wish to recover this value for their citizens by charging something like a market rate. But if local authorities were enabled to charge a market rate they would have an incentive to use public registers in ways that are outside the purposes of the register; there would be a conflict of interest with their role as custodians of registers.”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

²¹ This is the approach taken in some overseas legislation in respect of credit reference registers (although those would not usually be characterised as “public” registers). In some US states the individual is entitled under law to a free search each year or a search for no more than a set fee. Some laws, or proposed laws, also require that the charge made to the individual concerned not exceed the usual charge made to a customer of the credit reporting company.

Framework for Government-held Information which was finalised in 1997.²² Whether that approach appeals to public bodies outside the core state service, such as local authorities, would seem to be a matter for public policy formulation and the exercise of legislative and administrative powers. To the extent that this is a public register issue, it would seem undesirable to leave the matter solely to principle 4 and its reference to a “reasonable charge”.

7.8 PROPOSED NEW PRINCIPLE - bulk disclosures

7.8.1 It has been suggested that the existing principles do not get to grips with the full range of public register privacy issues and are therefore inadequate. The recommendations in respect of the four existing principles are intended to tackle their shortcomings and enhance their relevance and effectiveness. However, even with the recommended changes, there are significant privacy issues which for the most part remain unaddressed:

- there is patchy control of bulk searching of registers with resultant effects such as direct marketing and the creation of profiles on private databases;
- some registers are published in their entirety and sold, thereby ceasing to be under any effective control;
- although principle 3 does act so as to discourage bulk searching or copying of public registers, it does so indirectly and it does not openly confront and prohibit such practices.

The new principle I propose below seeks to address these problems.

Obtaining bulk information from a register

7.8.2 A constant refrain in submissions was the serious concern expressed at the release of bulk information from registers for commercial use – primarily direct marketing. The concerns expressed in submissions not only came from individuals or community groups, but also from the agencies maintaining public registers themselves. Particularly notable was the concern expressed by local authorities and organisations responsible for local government issues. A typical comment was made by Local Government New Zealand:

“Whatever for the most part the legal reasons may be whereby bulk information can be released for the commercial benefit of the recipients, such an outcome is clearly at odds with ... appropriate and laudable statutory purposes.”
(submission S51)

7.8.3 Certain registers have been revealed as having a commercial value and are subject to constant and continuing requests for bulk data which is used to create and sell lists which are used to direct market to the individuals concerned. One instance of this is found in respect of the use of the building consent register. Individuals who are erecting or altering a building must apply to their territorial authority for a building consent. Councils create weekly or monthly lists of the applications received and commercial interests regularly request these. As a result, the individuals who have applied for the consents receive, out of the blue, various solicitations to purchase building supplies, products or services. They have been given no choice. A number of territorial authorities have been reluctant to release such lists in deference to the privacy concerns of the individuals concerned but have been required to do so by the Ombudsmen. I have been consulted by the Ombudsmen on certain bulk requests and have opposed release on privacy grounds.

7.8.4 A similar issue arises in respect of the use of the valuation rolls or rates records whereby occupiers or absentee owners are approached by real estate agents. In June 1998 it was revealed that thousands of Auckland valuation records had

²² The full document is contained in a cabinet committee paper. The most easily accessible public version is to be found in the Law Commission, *Review of the Official Information Act 1982*, 1997 Appendix I.

been sold to a marketing company in Queensland, a jurisdiction having no privacy laws. In the first wave of marketing, Auckland property owners were the recipients of letters inviting them to “pay off your home loan four times faster without paying any more!!!” Press reports suggested “hard sell” tactics applied to those responding to the invitation. It was publicly reported that the bulk release of information, initially resisted by the department on privacy grounds, was prompted by the Ombudsmen’s office.²³ I had not been consulted on the matter by the Ombudsmen.

- 7.8.5 This issue has been canvassed in reviews of privacy law overseas. Several Canadian provinces have legislated to directly address the issue. For example, the Nova Scotia Freedom of Information and Protection of Privacy Act provides that a disclosure of personal information is presumed to be an unreasonable invasion of a third party’s personal privacy if:

“The personal information consists of the third party’s name together with the third party’s address or telephone number and is to be used for mailing lists or solicitations by telephone or other means.”²⁴

- 7.8.6 The Nova Scotia provision is repeated in other statutes. A new approach has been taken in a recent privacy law, the Freedom of Information and Protection of Privacy Act 1997 of Manitoba. That Act provides:

“Volume disclosure from a public register

The head of a public body shall not disclose to an applicant under this Part, personal information in a public registry on a volume or bulk basis.”²⁵

- 7.8.7 The Manitoba Act defines “public registry” as meaning a registry of information designated in regulations that is maintained by a public body and is available to the general public. It therefore closely resembles the concept of “public register” used in our own Act.

- 7.8.8 I consider that a principle modelled upon the Manitoba position would be a valuable addition to the public register privacy principles and directly address a problem which the other principles can only influence indirectly. However, I propose that it be modified by reference to the *purpose* for which a register is maintained - for example, to allow the accessing of the motor vehicle register to obtain hundreds of records relating to a faulty motor vehicle for a safety recall.

- 7.8.9 Accordingly, I suggest a principle which reads as follows:

PRINCIPLE 5

Bulk disclosures of information from public register

Personal information containing an individual’s name, together with the individual’s address or telephone number, is not to be made available from a public register on a volume or bulk basis unless this is consistent with the purpose for which the register is maintained.

- 7.8.10 The proposed principle is directed towards solicitation lists created directly from a register and therefore has features in common with the Nova Scotia provision. It is not an attempt to tackle the use of public registers to contribute public register profile details to mailing lists which already exist, because public

“The Committee believes that an individual’s privacy interest is not adequately protected where the person’s name, addresses, and telephone number can be made available for mailing lists. The Committee also objects to the use of public funds to finance access to information for private commercial purposes such as mailing list solicitation.”

- STANDING COMMITTEE ON THE ONTARIO LEGISLATIVE ASSEMBLY, REPORT ON THE MUNICIPAL FREEDOM OF INFORMATION AND THE PROTECTION OF PRIVACY ACT 1989, 1994

²³ “Ombudsmen order freed home details” *NZ Herald*, 26 June 1998.

²⁴ Freedom of Information and Protection of Privacy Act 1993 (Nova Scotia), section 20(3)(i).

²⁵ Freedom of Information and Protection of Privacy Act 1997(Manitoba), section 17(6).

register privacy principle 2 constrains that, to a certain extent, already. I have used the “volume or bulk basis” phrase from the Manitoba legislation. I believe that, for the most part, the agencies maintaining public registers generally have a good idea of the normal range of ordinary searches of the register. The marketing type requests are, I understand, relatively plain to identify, at least in respect of those registers currently facing such use. I have not framed the principle in terms of prohibiting the use of public registers for “direct marketing” although that may offer a satisfactory alternative.²⁶

7.8.11 The provision is similar to one very recently adopted in section 52(1)(f) of the Rating Valuations Act 1998 which allows regulations to be made:

“Prescribing limitations or prohibitions on the bulk provision of district valuation roll information for purposes outside the purposes of this Act or the Rating Powers Act or related legislation or to persons not having responsibilities in relation to the administration of this Act or the Rating Powers Act or related legislation.”

7.8.12 The principle also finds an echo in concerns recently expressed by the Electoral Select Committee over the purchase of electoral rolls and habitation indexes by businesses for marketing and debt collection purposes.²⁷

Publication of a register in its entirety

7.8.13 The discussion paper noted that there are circumstances in which a register may be dealt with, and disclosed, as a whole. For example, the agency maintaining the register might decide to publish the entire database as a book or in electronic form on CD-Rom. The publication may be made available for purchase so that anybody can possess the entire public register as at that point in time. An example is the electoral roll which is published at various points in the electoral cycle.

7.8.14 The discussion paper noted that some privacy risks arising from such publication include:

- the effect of disclosure may be multiplied over what would have been the effect of simply having the details placed on the register and available for a case by case search;
- the publication becomes available for use outside the control of the agency maintaining the register, for example, the entries can be electronically scanned into a database and used for profiling or marketing purposes;
- since many registers will be updated daily through additions and deletions, it is possible that printed versions in use may not be up to date;
- errors corrected on the official database will remain in printed copies earlier distributed;
- the complete version may be subject to re-sorting, or the addition of search references not intended or permitted for the original register.

7.8.15 The discussion paper canvassed the desirability of a principle prohibiting the publication or sale of a register in its entirety unless that publication or sale is necessary to achieve the purposes of the register. Considerable support for the proposal was offered in submissions. However, a number of submissions pointed out that the publication of a *significant portion* of a register would carry similar risks to publication of the *entire* register. I consider that the proposed principle will be satisfactory to address the concerns arising in relation to the publication or sale of entire or significant portions of registers as well as the bulk or volume searches for commercial purposes.

²⁶ The Act already has a definition of “direct marketing” in section 9 which could be utilised.

²⁷ Electoral Law Committee, *Interim Report on the Inquiry into the 1996 General Election*, April 1998, pages 32-33.

**RECOMMENDATION 91**

A further public register privacy principle should be enacted that provides that personal information containing an individual’s name, together with the individual’s address or telephone number, is not to be disclosed from a public register on a volume or bulk basis unless this is consistent with the purpose for which the register is maintained.

7.9 SECTION 60 - Application of information privacy principles and public register privacy principles to public registers

7.9.1 Section 60 requires every agency which is responsible for administering a public register to comply so far as reasonably practicable with the information privacy principles and the public register privacy principles. Where any such principle is inconsistent with any provision of any other enactment then, for the purposes of Part VII, that enactment will prevail.

7.9.2 The public register part of the Privacy Act is unusual in that it creates a regime that is not generally enforceable - although it may become so through the issue of a code of practice. Other sets of obligations created by the Act, such as in relation to the information privacy principles and information matching controls, can be taken on complaint to the Tribunal through the Act’s mechanisms.

7.9.3 It is also unusual that agencies which administer public registers are the only ones that need comply with the information privacy principles only “so far as is reasonably practicable”. Another unusual feature is that while public register privacy principle 2 applies to “any person”, this constraint upon use of personal information appears not to be enforceable like the general controls on use in information privacy principle 10.

7.9.4 In my view the position is unsatisfactory and anomalous. It is desirable for the application and enforceability of the public register controls to be brought more closely into line with the general approach of the Act. There were sound reasons in 1993 when the new public register regime was created to avoid a fully enforceable regime. However, that time is now past. To have the applicability of the principles, and remedies for aggrieved persons, put on a sounder basis will not in my view cause any significant difficulties. It would provide for a more satisfactory and effective regime for protecting privacy.

7.9.5 There are several approaches that could be taken to reforming this provision. For that reason, I will separately identify some of the problems or issues and suggest amendments which can be taken either as a package or as component parts. The key issues seem to concern:

- reconciling the application and savings provisions;
- reference to “every person” rather than “every agency”;
- use of “reasonable practicability” as the basis of an exception.

I address issues of enforceability at paragraph 7.10.

Application and savings provisions - sections 7, 8 and 60

7.9.6 The first issue to be addressed relates to the interaction between the savings provisions found in sections 7 and 60. Section 7(6) provides that:

“Subject to the provisions of Part VII of this Act, nothing in any of the information privacy principles shall apply in respect of a public register.”

7.9.7 Section 60, which is within Part VII, provides:

- in subsection (1), that the agency responsible for administering any public register must, in administering that register, comply “so far as is reasonably practicable” with the information privacy principles;

VII

s 60

251

“Our members were invited to comment to us on this review. Clearly the most important concern expressed was that public registers, particularly under the Building Act 1991 and the Rating Powers Act 1988, are being accessed by commercial organisations to obtain bulk information for direct marketing purposes. There is a widely held view amongst persons affected that this is a breach of their privacy.”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

- in subsection (3), that where any information privacy principle is inconsistent with any provision of any enactment then “for the purposes of this Part of the Act” that enactment shall, to the extent of the inconsistency, prevail.

7.9.8 I know from various dealings over the years, and from consultation, that this interaction is a point of confusion for people who have considered public register privacy issues. It seems to me that amendment of sections 7 and 60 is desirable to make the combined effect plainer. In my view this can be achieved, in a straightforward manner, by several minor changes, the first of which involves substituting for section 7(6) a provision to read:

“The information privacy principles apply in respect of a public register to the extent specified in section 60 and section 63(2)(b).”²⁸

This of itself should not make any significant substantive difference to the way that the Act applies in this context. The new provision will primarily act as a flag in relation to the primary section. The subsection should probably be relocated into section 8 as it concerns the application of the principles rather than the saving of other laws.



RECOMMENDATION 92

Section 7(6) should be replaced with a subsection in section 8 providing that the information privacy principles apply in respect of a public register only to the extent specified in section 60 and 63(2)(b).

7.9.9 The second set of minor changes concern section 60 itself. The first point to note is that section 60(3) ties in directly with section 60(1), a point obscured somewhat by the interposition of subsection (2). A redraft should bring those two provisions together. Accordingly, the phrase “subject to sub-section (3) of this section” can be dropped (which is consistent with drafting changes adopted by the Parliamentary Counsel Office). It may be possible to re-draft section 60(3) more plainly. It would be desirable to drop the phrase “so far as is reasonably practicable” so as to more closely align the regime to that applying elsewhere in the Act.

7.9.10 Subsection (2) of section 60 provides that:

“Every person shall, so far as is reasonably practicable, comply with principle 2 of the public register privacy principles.”

“Every person” includes bodies which are exempted from the definition of “agency”. In my view, the words “every person” could be replaced with “every agency” in section 60(2) without creating any significant new privacy risks. I believe it is better that the relevant bodies be able to take the benefit of their usual exemption to the use controls of the Privacy Act.

7.9.11 Section 60, following these suggestions (and I make further suggestions below) could then be amended as follows:

- (1) Omit “subject to subsection (3) of this section” and “so far as is reasonably practicable”.
- (2) Subsection (1) does not apply where any information privacy principle or any public register privacy principle is inconsistent with any enactment and, in that event, the enactment prevails to the extent of the inconsistency.
- (3) The present subsection (2) - which could alternatively be subsection (1) - substitute “any agency” for “any person”.

²⁸ The reference to section 63(2)(b) encompasses the position established by a public register code of practice.

**RECOMMENDATION 93****Section 60 should be amended as follows:**

- (a) in subsection (1) omit the phrases “subject to subsection (3) of this section” and “so far as is reasonably practicable”;
- (b) the content of subsection (3) should be moved adjacent to subsection (1) and redrafted in plainer fashion;
- (c) in subsection (2) “person” should be replaced by “agency”.

“Reasonably practicable” in section 60(2)

7.9.12 A further issue with subsection (2) is that difficulties could arise in relation to a use or disclosure complaint against an agency (other than an agency which administers a public register) if the action complained about involved a breach of public register privacy principle 2. For example, the agency may claim that there was an issue as to whether compliance was “reasonably practicable”. While relevant to the breach of the public register principle that phrase does not constitute an exception to either the use or disclosure principles.

7.9.13 In any case, it is not clear that “reasonable practicability” makes for a suitable exception relating to compliance. If exceptions are necessary it would be better, in my view, for these to be based upon specified public interests or individual authorisation as is the case with the exceptions to the information privacy principles. In my view the reference to “as far as is reasonably practicable” should be replaced by a reference to authorisation by the individual concerned and disclosure to that individual. Other public interests, if any, would be reflected in other legislation, the effect of which is saved by section 60(3).

**RECOMMENDATION 94****Section 60(2) should be amended:**

- (c) by omitting the words “as far as is reasonably practicable” and
- (d) by substituting an exception based upon the authorisation of the individual concerned.

7.10 SECTION 61 - Complaints relating to compliance with principles

7.10.1 Section 61 provides for complaint-initiated, or Commissioner-initiated, inquiries and investigations where it appears that:

- a public register provision is inconsistent with any of the information privacy principles or public register privacy principles;²⁹
- an agency administering any public register is not complying with the information privacy principles or public register privacy principles;³⁰
- any person is not complying with public register privacy principle 2.³¹

7.10.2 The Commissioner is given powers to carry out the inquiry or investigation which can result in a report to the chief administrative officer of the agency subject to the inquiry or investigation and may include recommendations for taking action to ensure greater adherence to the principles. It is clear from section 66 that such an inquiry or investigation cannot lead to proceedings before the Tribunal. However, if a code of practice is issued Tribunal proceedings can be taken in respect of certain actions which constitute a breach of that code.

7.10.3 There have been few complaints investigated under the public register privacy principles. There is little awareness yet of the existence of the principles or complaints mechanisms although expressions of dissatisfaction continue to ar-

²⁹ Sections 61(1), (2).

³⁰ Section 61(3)(a), (4).

³¹ Section 61(3)(b), (4).

rive at my office from individuals who are annoyed at receiving targeted marketing approaches using personal information obtained from registers. Although one inquiry is under way, most such matters have not led to formal investigations because:

- complainants lose interest when learning that complaints under section 61 can, at most, lead to a recommendation and not a remedy;
- complainants realise, after discussion with the Commissioner’s enquiries officers, that actions authorised or required by other legislation cannot be prevented by the operation of the principles.

7.10.4 In relation to section 60³² I canvassed the issue of whether the enforcement of the public register regime should be brought more closely into conformity with the approach taken to compliance with the information privacy principles by agencies generally. My recommendation is that the regime becomes fully enforceable in respect of agencies which administer public registers, and, in respect of principle 2, “any agency”. If my recommendation is not accepted then principle 2 should, as a minimum, be made enforceable in respect of any agency other than the agencies which administer the relevant public registers.

7.10.5 If all or some of these recommendations are accepted some resultant change will be necessary to section 61. In my view, it should be possible to amend section 61 to bring complaints or investigations under subsection (3) into the mainstream of the Act’s complaints mechanisms whereby matters could, if appropriate, be taken to the Complaints Review Tribunal. Most submissions supported this.³³ I consider that it would be inappropriate to do the same for subsections (1) and (2) since complaints of that type involve an inquiry into a provision in an enactment and may conclude with a recommendation as to the desirability of legislative action. These would be inappropriate functions for a judicial tribunal.

7.10.6 If the public register regime is to become enforceable it would generally be desirable, in my view, for this to be done by bringing the matters into the mainstream of the complaints mechanisms rather than creating further specific complaints procedures applicable solely in relation to public registers. Accordingly, in addition to any amendment to section 61 there will also be a need for consequent amendments to be made to certain other aspects of Part VIII which deals with complaints.



RECOMMENDATION 95

The public register privacy principles should be enforceable in a similar manner to the information privacy principles by amending, as necessary, sections 61(3) - (5) and 66.

7.11 SECTION 62 - Enforceability of principles

7.11.1 If complaints relating to public registers are brought into the “mainstream” with regard to enforceability and Tribunal proceedings, then it is possible that section 62 could be appropriately moved into section 11.

7.12 SECTION 63 - Codes of practice in relation to public registers

7.12.1 Section 63 provides for the Commissioner to issue codes of practice in relation to public registers. A code may modify the application of the public register privacy principles or the information privacy principles by prescribing stand-

³² See paragraph 7.9.2 and 7.9.4.

³³ Seven of the 9 submissions on the question agreed that complaints or investigations under section 61(3) ought to be able to be taken to the Tribunal (see submissions T1, T5, T6, T9, T12, T15 and S36). Submissions T17 and S42 did not support the proposition.

ards that are more stringent or less stringent than prescribed by those principles, or by exempting any action from any such principle, either unconditionally or subject to conditions that are prescribed in the code. A code may also prescribe how any one or more of the public register or information privacy principles are to be applied or are to be complied with or may “impose requirements that are not prescribed by any public register privacy principle”. A code may also provide for review and expiry. Procedures set out in sections 47 to 52 for Part VI codes are followed with any necessary modification.

- 7.12.2 Section 63(4) provides that to the extent that any public register code is inconsistent with any provision of any enactment, the code shall, to the extent of the inconsistency, be of no effect. This follows normal rules of statutory interpretation and would undoubtedly be the case even if subsection (4) had not been included. It is also consistent with the approach taken in sections 7 and 60 in relation to the status of the privacy principles as against other laws. However, subsection (4) is an important reminder as to the limits of what may be achieved by a code of practice particularly in the area of public registers where there is always another enactment - the one establishing the register - to take into account.
- 7.12.3 Given the significant privacy risks that I have outlined in relation to public registers it may be surprising that no public register codes of practice have been issued over the last four years. Reasons why no codes have been issued include:
- a code will be of no effect if inconsistent with other legislation - this has meant that it has been difficult to pursue effective codes which get to grips with the privacy issues where there appears to be a statutory obligation upon a registrar to give access to information without any discretion to withhold information for reasons of privacy;
 - even where the statutory interactions between the Privacy Act and the public register provision can be resolved there sits, in the background, the Official Information Act and the Local Government Official Information and Meetings Act which have the potential to undermine the approach taken by a code;
 - there has been the need to develop experience in the issues, and a coherent approach, which I believe my office now possesses;
 - other priorities have prevented significant resources being directed to the issues.
- 7.12.4 Although no code has been issued, preliminary work has proceeded on two prospective codes touching upon public register issues, including:
- a proposal for a code addressing the motor vehicle register - which was a spin-off from an earlier proposal for a broadly based law enforcement code which did not eventuate;
 - a proposed credit reporting code - which would require consideration of the issue of credit reporting companies utilising public register sources of information.
- 7.12.5 A credit reporting code proposal remains under consideration. Although considerable work was done on a proposed motor vehicle register code, progress was uneven. In 1997 work was discontinued on the code by my office and the LTSA and Ministry of Transport due to the opportunity to pursue privacy issues in relation to the motor vehicle register through primary legislation. This experience has been typical of a number of public register issues. It may be more straightforward, and ultimately more effective, to pursue matters through primary legislation where the opportunity exists than it is to seek to develop a code which may only be able to tinker at the edge of the privacy issues if the public register provision is at variance with a privacy solution.
- 7.12.6 Legislative reform of certain provisions establishing public registers or statutory

registers has been undertaken over the last four years. Some sound models for the reform of other register provisions have been enacted. The resultant provisions have either effectively addressed privacy issues or created an environment where, if necessary, a code of practice can usefully be issued.

- 7.12.7 A number of amendments to public register provisions made over the last five years have been mentioned elsewhere in this part of the report in relation to each of the public register privacy principles. However, I will mention here two examples where the resultant provisions acknowledge the possibility of a code of practice.
- 7.12.8 The first example is section 122ZI of the Local Government Act 1974. That provision created a new public register and set out the appropriate search references. However, in order to anticipate the possibility of the need to change search references at some future point the provision provided for the specifying of further search references by regulation. The section provided, as an alternative, that search references could be specified by code of practice. Therefore there will be no inconsistency with the statute if a code specifies further search references.
- 7.12.9 In respect of the Domestic Violence Act 1995 there is provision for aspects of the regime, such as the forms to be used, governing non-publication of information relating to protected persons to be spelt out by regulations or Privacy Act codes. In the broadly based Domestic Violence Act regime, which can apply to a large number of registers, it is possible that regulations might be issued specifically in respect of some registers, while others might be subject to a code of practice. The balance of the registers may find it entirely satisfactory to operate administratively without the need for aspects to be prescribed by either regulation or a code of practice.
- 7.12.10 It is anticipated that the most likely circumstance where the matters mentioned in the Local Government Act or Domestic Violence Act would warrant being effected by code of practice is where a code of practice is justified on privacy grounds anyway. The matters under consideration can then be incorporated into the relevant code of practice. The resultant code would be a combination of one issued under section 63 which is supplemented by the additional matters that can be done in those other provisions. I understand that I have powers to issue “combined” codes of practice of that type as was the intention when those provisions were passed.

7.13 SECTION 64 - Effect of code

- 7.13.1 Section 64 provides that where a code of practice in relation to a public register is in force, any action that would otherwise be a breach of a public register or information privacy principle is deemed not to be such a breach for the purposes of Part VII if done in compliance with a code of practice. Conversely, failure to comply with a code, even if it is not otherwise a breach of a public register privacy principle, is deemed to be a breach of a public register privacy principle.
- 7.13.2 This is similar to section 53 which states the effect of a code of practice issued under section 46. However, the importance of section 64 is that under current arrangements a code can put in place an enforceable regime whereby complaints can be taken to the Tribunal. In this respect the present regime differs from that in relation to codes issued under Part VI.³⁴

³⁴ The position is similar to that which applied in respect of Part VI codes during the transitional period following the introduction of the Act. See Privacy Act, section 79(3).

7.14 SECTION 65 - Power to amend Second Schedule by Order in Council

7.14.1 Section 65 provides for the addition of new public register provisions to the Second Schedule. The amendment is by way of Order in Council upon the advice of the Minister of Justice after consultation with the Privacy Commissioner.

7.14.2 In the five years to July 1998 the Order in Council route has not been used. Since the question of adding registers to the list has arisen during that period in the context of legislative proposals to create new registers, or amend the legislation governing existing registers, the Second Schedule has simply been amended by statute. However, in the light of the preceding discussion I am now of the view that a more systematic approach should be taken to bringing existing registers within the public register controls. The use of Orders in Council will provide a convenient mechanism to achieve this.

Use of Orders in Council to bring statutory registers into scheme

7.14.3 To bring all, or most, of the existing statutory provisions creating registers open to public search into the Second Schedule will require a process of:

- *identification* - locating the existing provisions in enactments;
- *evaluation* - considering, in conjunction with the agencies affected, any case for excluding a register from the regime;
- *making the order* - the process of preparing the order, consulting in relation to its wording, and finally issuing it;
- *implementation* - ensuring the new requirements are satisfactorily brought into effect.

7.14.4 I do not expect that the task of identifying the relevant provisions will be difficult. Many register provisions are amenable to straightforward computer searches of an electronic legislation database. Some obscure provisions may be overlooked at the early stages of any identification project but this, in itself, does not carry significant privacy risks.

7.14.5 The process of evaluation will be somewhat time consuming on the part of both my office and the Ministry of Justice. However, I am confident from experience since 1993, and examination of the issues in the course of this review by my office and the Ministry, that few significant problems should be encountered. The main challenge will be to engage the agencies which administer the registers in considering the issues, and to work through any implications for their registers. Many such agencies may have had no call previously to study the public register privacy principles and, human nature being what it is, will be cautious at the prospect of any set of statutory controls bearing upon them. However, I have found amongst officials who maintain statutory registers, a genuine interest in privacy issues and most are respectful of the privacy of people whose data they are entrusted with. Study of the matter by my office and the Ministry has not found any clear basis for the exclusion of any class of statutory registers from the scheme, but any agency would be free to make a case to keep its register outside the controls.

7.14.6 There is no need to have a single Order in Council to add all identified registers to the Second Schedule in one go. It would make most sense to undertake the task in batches. I suggest that the first Order in Council ought to be issued within 12 months of the start of the project of identification, with the whole task completed within two years. The nature of the grouping of registers in the Order in Council is not important from a legal or privacy perspective but would be a practical matter for the Ministry of Justice. However, there may be practical implementation issues which favour batching of Orders in Council by administering department or subject matter.

“It is submitted that statutory registers inherently can pose the same privacy concerns or risks as public registers. Such registers should therefore, be included in the Second Schedule to the Privacy Act 1993. This will ensure that there are privacy safeguards in place where any enactment, under which statutory registers are created, provides a discretion as to the purposes for which the information is to be used or released.”

- NURSING COUNCIL OF NEW ZEALAND, SUBMISSION T15

- 7.14.7 The last consideration is implementation of the public register controls within the agencies maintaining the new public registers. The process of consulting agencies in the preparation of the Order in Council will, I expect, quite effectively begin the compliance process. Ideally the Ministry of Justice will provide explanatory materials to the departments whose registers are proposed to be brought within the scheme. In the process of consultation those departments will begin considering the implications of the principles for their register and operation. The implications will be relatively modest and may not require immediate changes in practice in many cases. The Orders in Council should allow sufficient time before coming into effect to provide for any necessary operational changes.
- 7.14.8 The bringing of the additional statutory registers into the public register regime will provide an opportunity for timely general public education. For example, the ability for individuals who have a protection order under the Domestic Violence Act to obtain suppression directions on a significant range of registers is a matter that will need some co-ordinated information. The relevant advice needs to be available to professional advisers since individuals in such distressing situations are unlikely to know the full details themselves.

**RECOMMENDATION 96**

The Order in Council process in section 65 should be utilised to add existing register provisions in enactments to the list in the Second Schedule. The Ministry of Justice should commence work to identify the relevant enactments, and to consult with the relevant agencies, so that the first Order in Council is ready to be issued during the 1998/99 year with the completion of the project by the end of the following year.

Domestic Violence Act regulations

- 7.14.9 One of the issues that will need to be considered when further provisions are being added to the Second Schedule is whether the registers should also be brought within the scheme provided in Part VI of the Domestic Violence Act 1995 for the non-publication of information relating to protected persons on public registers.
- 7.14.10 This involves a consideration of separate issues to those involved in the decision to add a register provision to the Second Schedule. It should not be assumed that because a register is created as a “public register” it automatically follows that the domestic violence regime should apply. The critical reason to add a register to the domestic violence regime concerns whether an individual’s current whereabouts can be traced using the register. This primarily involves registers which display residential addresses. However, it may also be an issue for registers maintained on a district basis where appearance on a register indicates likely residence in that district (allowing further enquiries to pinpoint the location). In respect of existing public register provisions it has already been determined that it is unnecessary to add the drivers licence register to the domestic violence regime since it does not permit the location of individuals.
- 7.14.11 It would seem sensible for the question of the applicability of the Domestic Violence Act to be gone into in conjunction with the project to bring registered provisions within the Second Schedule.

**RECOMMENDATION 97**

The Ministry of Justice should, in carrying out the exercise to bring register provisions into the Second Schedule pursuant to section 65, also consider in respect of each register the desirability of issuing regulations under section 121 of the Domestic Violence Act 1995.

7.15 STATUTORY MECHANISMS FOR SUPPRESSION OF DETAILS ON REGISTERS

7.15.1 As will be apparent from this chapter, it is a difficult task to craft privacy provisions which can work in tandem with public registers. Generally a satisfactory approach will be one that reconciles the privacy interests with legitimate competing interests requiring disclosure of personal information. The approach I have generally advocated in this chapter has been to establish public registers with clearly stated purposes and to use controls, such as search references, to ensure that access is only given consistently with those purposes. However, sometimes there will be a need for an absolutely open and unrestricted search right and it is necessary to consider other safeguards in that context. One approach is to recognise that certain people have a particular need to have some of their details suppressed from general public search. A common example is the residential address of persons who have good reason to fear violence if they are located by a person who poses a real threat to them.

7.15.2 In any case, even where a regime has been fashioned to ensure that searches are only given for people having a legitimate “need to know” particular information, there may nonetheless be a case for a fall-back protection for people at risk. After all, it will be little comfort to a person who has been tracked down and attacked to know that the perpetrator may be prosecuted for having given a false declaration. Most of the chapter has been directed towards a regime that works reasonably well in a majority of cases to protect reasonable expectations of privacy. Where it comes to personal safety or harassment it is sometimes necessary to establish even stronger safeguards.

Suppression mechanisms in existing statutes

7.15.3 A suppression option has been adopted in several New Zealand statutes. The first example of which I am aware was the insertion in 1980 of section 62A into the Electoral Act 1956. This allows a person to enrol to vote but not to be named in the published electoral roll if that would be “prejudicial to the personal safety of the person or his family”. The provision has been carried over to section 115 of the Electoral Act 1993. A similar step was taken in section 19(5) of the Transport (Vehicle and Driver Registration and Licensing) Act 1986 to enable details to be withheld for reasons of “privacy or personal safety”. Suppression regimes exist in relation to registers open to public search maintained under the Radiocommunications Act 1989 and the Fisheries Act 1996. Sometimes other interests such as a fear of harassment, desire to preserve privacy, or national security, are specified.

7.15.4 Most significant of all such provisions are those contained in Part VI of the Domestic Violence Act 1995. A person who has obtained a protection order under that Act can apply for a direction from the agency which maintains a public register that identifying information on the register not be made publicly available. An elaborate set of provisions sets up the mechanism and allows for complaint to the Privacy Commissioner where an application for a direction is refused.

7.15.5 The provisions in the Domestic Violence Act can, in appropriate cases, be extended to any register maintained pursuant to a public register provision identified in the Second Schedule to the Privacy Act. Nonetheless there remain significant limits in protection of vulnerable people. The Domestic Violence Act, as its name suggests, only covers persons who have been the subject of, or fear, *domestic* violence. There are other people who have reason to fear violence if their whereabouts are easily able to be traced. These include, for instance, people, such as judges and police officers, whose occupation may bring them into contact with violent people. Witnesses and jury members may also sometimes be the subject of threats. Another group of people who might, in appro-

“Suppression of information which endangers a person’s safety does need to be addressed. The Domestic Violence Act provisions address part of the issue but we would value some provision to give us discretion to respond to an individual’s fear for their safety - an ability to block information on registers while other protections are put in place; a right to err on the side of caution.”

- FRANKLIN DISTRICT COUNCIL,
SUBMISSION T2

priate cases, benefit from being able to obtain a suppression direction are those who have been the subject of harassment.³⁵

Harassment

- 7.15.6 In my report on the Harassment and Criminal Associations Bill I suggested that consideration should be given to enabling people who obtain a restraining order under the Harassment Act to obtain a direction for suppression of details held on a public register in a manner similar to the scheme operated under the Domestic Violence Act.³⁶ In my report, I went through the issues in some detail and suggested that the objective might be achieved in one of three ways:
- (a) amend the Electoral Act and other specific provisions only;
 - (b) extend the Domestic Violence Act scheme to victims of harassment;
 - (c) tackle the issue more comprehensively.
- 7.15.7 There were pros and cons in relation to each of the options. Amending solely the Electoral Act would mean that the issue was only partially addressed. Extending the Domestic Violence Act scheme to victims of harassment would be confusing conceptually since it would treat a restraining order under the Harassment Act as a protection order for the purposes of Part VI of the Domestic Violence Act. Tackling the issue more comprehensively raised its own difficulties since it might involve discontinuing the Domestic Violence Act scheme which had only recently been created. The comprehensive approach also raised issues which were beyond the remit of the select committee studying the Harassment and Criminal Associations Bill.
- 7.15.8 The select committee studying the Harassment and Criminal Associations Bill adopted the first option and solely amended the Electoral Act. In doing so the Committee reported:

“The Privacy Commissioner expressed concern that victims who apply for restraining orders need their privacy protected, especially their home address and phone number. These details can be disclosed on public registers such as those under the Electoral and Births, Deaths, and Marriages Registration Acts.

“Section 115 of the Electoral Act 1993 allows the Chief Registrar to direct that a person’s name not be included on the electoral roll where publication would be prejudicial to his or her personal safety. Where a protection order under the DVA is enforced it is sufficient to produce the order, without having to produce any further evidence. The proposed restraining orders under the provisions in the Bill have a similar effect. Therefore, we recommend [a] new clause to amend the Electoral Act 1993 so that a restraining order made under the provisions in the Bill will be sufficient to justify the protected person’s name being placed on the unpublished roll.

“We note that the Privacy Commissioner suggested adapting Part VI of the DVA to enable people who obtain restraining orders to get directions that their personal details contained in public registers be held in a confidential list. We understand that as part of the Privacy Commissioner’s review of the Privacy Act 1993, a discussion paper will be

³⁵ Note that harassment does not always involve violence and is therefore not necessarily subsumed into any personal safety ground.

³⁶ See Report by the Privacy Commissioner to the Minister of Justice on the Harassment and Criminal Associations Bill (other than provisions dealing with interception warrants), 23 January 1997.

released in the near future relating to the public register provisions in the DVA. The discussion paper may make a recommendation that will affect Part VI of the DVA. Therefore, it seems preferable to *defer the decision* of incorporating a regime similar to that in the DVA until the outcome of the discussion paper is known. We consider it a preferable alternative to recommend the *interim measure* as outlined above.”³⁷ [Emphasis added]

- 7.15.9 I have taken the select committee’s report, particularly the portions highlighted, to indicate that they saw the amendment to the Electoral Act as an interim measure pending consideration of the merits and workability of some broader solution concerning suppression of details of persons who have obtained a restraining order. The committee rightly noted that as part of my review of the Privacy Act I would release a discussion paper relating to these issues.

Discussion paper

- 7.15.10 In the discussion paper the problem of people who feared violence, but who did not have a protection order, and those who had been a subject of harassment were outlined. Two questions were posed. The first asked:

“Should there be a public register privacy principle dealing with suppression of information in cases where it is established that an individual’s safety, or that of their family, will be put at risk through the availability of details of their whereabouts?”

- 7.15.11 Fourteen submissions were received. Ten answered yes³⁸ while only two answered no.³⁹ Two submissions did not directly answer the question but offered observations. One, from a district council, noted that the issue of personal safety needed to be addressed, that the Domestic Violence Act addressed only part of the issue, and the Council would value having a discretion to respond to an individual’s fear for their safety - “an ability to immediately block information on registers while other protections are put in place; a right to err on the side of caution.”⁴⁰ The other suggested a need to be cautious about extending Part VI of the Domestic Violence Act further before it had an opportunity to operate in practice for a while.⁴¹

- 7.15.12 A second question asked:

“As an alternative, or supplement, to creating a new principle dealing with personal safety, should Part VII of the Privacy Act contain mechanisms for obtaining suppression directions on public registers which would replace Part VI of the Domestic Violence Act but be applicable to a wider range of circumstances?”

- 7.15.13 As with the previous question, 14 submissions were received. Nine directly answered yes.⁴² No submissions answered no to the question. The other sub-

³⁷ Harassment and Criminal Associations Bill as reported from the Justice and Law Reform Committee, commentary, page vi. The Electoral Law Committee also supported the change. See Report of the Electoral Law Committee, *Interim Report on the Inquiry into the 1996 General Election*, April 1998, page 34.

³⁸ See submissions T1, T3 - T6, T9, T11, T12, S36 and S51. T4, T11 and S51 answered this question, and the following one, jointly in the affirmative.

³⁹ See submissions S42 and S58.

⁴⁰ Submission T2.

⁴¹ Submission T17.

⁴² See submissions T4, T5, T6, T9, T10, T11, S42, S51 and S58. T4, T11 and T51 answered the two questions jointly in the affirmative.

missions generally offered observations on the proposal but without opposing the course of action suggested. One expressed a preference for this proposal rather than the creation of a public register privacy principle as suggested in the previous question.⁴³ Another preferred mechanisms of the type contemplated in the question to be a supplement to a principle.⁴⁴ Others were unsure of the merits of one approach as against the other.⁴⁵

- 7.15.14 In my view, the issue should be taken forward. The two mechanisms canvassed in the discussion paper were the creation of a new public register privacy principle or the creation of a broadly based scheme for the obtaining of directions for suppression, modelled upon the Domestic Violence Act. A third possibility, anticipated in the second question, is to do both - create a new principle and use a suppression mechanism as a supplement. I have decided to recommend this third option.
- 7.15.15 I believe that a public register privacy principle and a statutory suppression scheme together will achieve more than simply doing one thing or the other. A principle, for example, will apply to all public registers listed in the Second Schedule whereas the suppression mechanism will be applied on a case by case basis only where appropriate. Sometimes the personal safety issues can be dealt with adequately without the need for the statutory suppression scheme. The statutory suppression scheme will prevail over inconsistent public register provisions whereas a principle will not.⁴⁶
- 7.15.16 In this report I do not set out all the detail of how this arrangement would operate. If a decision is taken by the Government to implement my recommendation there will be important work to be done on the detail and I will offer further views during that process. However, I outline the new principle that I propose and sketch out the broad details of how a broadly based statutory suppression scheme could be created.

Proposed new public register privacy principle

- 7.15.17 In devising a new principle directed to personal safety issues I have considered the Council of Europe Recommendation R(91)10 which I am directed to have regard to under section 13(1)(e) when reviewing the public register privacy principles. Clause 2.2 of those recommendations states:

“Unless domestic law provides appropriate safeguards and guarantees for the data subject, personal data or personal data files may not be communicated to third parties for purposes incompatible with those for which the data were collected.”

- 7.15.18 This provision does not explicitly refer to personal safety issues and, in a sense, simply restates the general approach to privacy issues. However, it does point out two things, the need for “safeguards” to be taken, and the point at which the risk is manifest, the communication of personal information to third parties for purposes incompatible with those for which the information was collected. Part 3 of Recommendation R(91)10 provides an approach for “sensitive data”. Strictly speaking this is not directed to data giving rise to risks of personal safety but instead to those categories referred to in article 6 of the Council of Europe Convention No 108.⁴⁷ However, it may suggest an approach when it states:

⁴³ See submission T9.

⁴⁴ See submission S42.

⁴⁵ See, for example, T1 and S36.

⁴⁶ See section 60.

⁴⁷ Article 6 refers to personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, and data relating to criminal convictions.

“Sensitive data

3.1 Personal data falling within any of the categories referred to Article 6 of Convention 108 should not be stored in a file or in part of a file generally accessible to third parties.

Any exception to this principle should be strictly provided by law and accompanied by the appropriate safeguards and guarantees for the data subject.”⁴⁸

7.15.19 Accordingly, I have devised a new public register privacy principle which directs agencies maintaining public registers to keep certain details stored separately from information generally accessible to third parties with an exception where appropriate safeguards are in place. Agencies should have a process whereby individuals with special safety concerns can ask to have the details of their whereabouts held in a non-accessible part of the database. Those details would only be released with a great deal of care to ensure that the information was not to be used for an incompatible purpose. An agency would not need to segregate such details if appropriate alternative safeguards addressed the risks involved. The proposal would not require *all* information to be held separately, only that revealing an individual’s whereabouts.

7.15.20 The proposed new principle might appear along the following lines:

*PRINCIPLE 6**Personal safety or harassment*

- (1) Where practicable, personal information revealing an individual’s whereabouts should not be stored in a part of a register generally accessible to the public where it is shown, on an application by the individual to the agency maintaining the register, that the individual’s safety or that of the individual’s family, would be put at risk through the disclosure of the information.
- (2) An agency maintaining a public register shall have reasonable procedures to invite, evaluate and determine applications by individuals whose personal safety may be put at risk by disclosure.
- (3) It is an exception to clause (1) of this principle where other appropriate safeguards are taken to ensure that the information is not disclosed to the public for purposes unrelated to the purposes for which the information was collected or obtained.

7.15.21 I consulted on the *proposition* that there be such a principle but not on the draft principle itself set out above. The detail of the approach to be taken, and the drafting of the provision, would need to be the subject of consultation with agencies maintaining public registers. Accordingly, I have framed my recommendation in terms of the adoption of a suitable principle rather than the adoption of the actual principle suggested above. There may be other satisfactory ways of drafting a principle to achieve a similar purpose.

“Most state legislation in Australia contains express provisions that residential address is not to be part of the register of nurses available for inspection by the public.”

- NURSING COUNCIL OF NEW ZEALAND, SUBMISSION T15

⁴⁸ Clause 3.2 is not relevant for present purposes relating to the making available of sensitive categories of data, as outlined in Convention No 108, concerning public figures.

**RECOMMENDATION 98**

A new public register privacy principle should be created which obliges agencies maintaining public registers to adopt a process to hold details of an individual's whereabouts separately from information generally accessible to the public where it is shown that the individual's safety or that of the individual's family would be put at risk through the disclosure of the information. An exception is to be provided where alternative safeguards exist to ensure that such information is not disclosed to the public for purposes unrelated to the purposes for which the information was collected or obtained.

Mechanism for obtaining suppression directions

- 7.15.22 Over the last few years my office has made a number of suggestions for improving individual public register provisions as they come up for enactment or re-enactment. Often the best solutions, which provide for a free flow of information for legitimate uses but otherwise gives adequate privacy protection, are crafted in relation to particular registers in their own special circumstances. However, a register-by-register approach is inadequate to fully address either privacy or personal safety concerns. Unless some minimum privacy and personal safety protections are established across the board in relation to registers, the very good regimes established in one context may be undermined by the lack of safeguards in others. For example, an abusive partner may go to extraordinary lengths to seek to trace an estranged partner. It will not be sufficient to provide protection in relation to the electoral roll and motor vehicle register if, knowing the partner's assets, affiliations and personal interests, the violent person can nonetheless trace the individual easily through other registers.
- 7.15.23 In suggesting the regime now established in the Domestic Violence Act I was inspired by a scheme that had been conceived, but not implemented, in New South Wales. The Privacy and Data Protection Bill 1994 in that State proposed a very simple clause to establish a generic suppression regime. It stated:

“Suppression of information

- 20(1) A person about whom personal information is contained, or proposed to be placed, on a public register may apply to the record-keeper to have the information removed from, or not placed on, the register as publicly available and not disclosed to the public.
- (2) However, information that is removed from, or not placed on, the register as publicly available is to remain on the register for other purposes.
- (3) Despite the provisions of any other Act, the record-keeper may agree to the application if the record-keeper is satisfied that suppression of the information would not unduly compromise the register and the record-keeper is also satisfied that the applicant's safety or the safety of members of the applicant's family may be at risk if the application is not granted.
- (4) An applicant who is aggrieved by a decision of a record-keeper under this section may complain to the Privacy Commissioner under section 23.
- (5) In dealing with the complaint, the Privacy Commissioner may recommend that the record-keeper agree to the application or may notify the complainant that, in the Commissioner's view, the application was properly refused.
- (6) A record-keeper must comply with a recommendation by the Privacy Commissioner under this section.”

- 7.15.24 That simple provision provides an interesting contrast with the 17 section Part



VI of the Domestic Violence Act.⁴⁹ The New South Wales provision has not been implemented and therefore it cannot be known whether it would have worked satisfactorily without the degree of detail set out in the New Zealand Act and Regulations. Nonetheless, the degree of detail in the Domestic Violence Act serves as a warning as to the need to avoid unduly further complicating matters. Furthermore, I am keen to maintain the Privacy Act as “user friendly” as possible and would wish to achieve the objective with the least complexity possible.

7.15.25 Being mindful of issues of complexity, the desirability of avoiding duplication and the need for effective protection, I have concluded that the following features would probably make for the most effective and straightforward regime:

- a single generic suppression regime which is located in an appropriate statute - this leads me to recommend that the existing Domestic Violence Act regime be subsumed in a generic scheme to be in the Privacy Act;⁵⁰
- the Domestic Violence Act regime should remain as far as possible unchanged albeit relocated into another statute;⁵¹
- the detail of the scheme, presently found in Part VI of the Domestic Violence Act, to be placed in a schedule to the Privacy Act rather than in Part VII of the Act itself;⁵²
- opportunities should be taken to simplify some of the provisions from the Domestic Violence Act scheme - primarily in relation to links to the Privacy Act’s Second Schedule and complaints processes;
- directions for suppression should cover circumstances presently contemplated by the Domestic Violence Act (evidenced by individuals having obtained protection orders) and extend to other personal safety and harassment cases - with harassment cases being substantiated by the production of a restraining order and others substantiated in some suitable manner such as is provided for in section 113 of the Electoral Act 1993.

7.15.26 A number of practical and consequential issues would need to be worked through in transferring the regime from the Domestic Violence Act and satisfactorily providing for other cases of personal safety and harassment. For example, existing regulations may need to be carried over in some way. It would also make sense for the Second Schedule of the Privacy Act to be reformatted so that it is clear at a glance which public register provisions have also been brought within the suppression regime.



RECOMMENDATION 99

A mechanism should be established in Part VII of the Act, with the details set out in a new schedule, enabling individuals to obtain suppression directions in relation to public registers which would replace Part VI of the Domestic Violence Act but be applicable to a wider range of circumstances concerning personal safety and harassment.

7.16 INTERACTION WITH OFFICIAL INFORMATION ACT AND LOCAL GOVERNMENT OFFICIAL INFORMATION AND MEETINGS ACT

7.16.1 I cannot conclude the discussion of public registers without noting that the

⁴⁹ Part VI of the Domestic Violence Act also has to be read in relation to relevant regulations. The Domestic Violence (Public Registers) Regulations 1996 runs to 14 clauses and a schedule.

⁵⁰ I see the Domestic Violence Act and Harassment Act as inappropriate places to locate a generic regime as did officials advising the select committee on the Harassment and Criminal Associations Bill. A suitable alternative, but beyond my terms of reference, would be to create a stand-alone statute. One shortcoming of a stand-alone statute would be continuation of some complexity in cross referencing to the Privacy Act’s Second Schedule and my complaints jurisdiction.

⁵¹ This should offer least disruption to agencies maintaining public registers.

⁵² This should offer least disruption to regular users of the Privacy Act.

“Our members strongly share the concern about individual privacy. However, as managers of various public registers they have little option under the present law and administrative arrangements but to disclose bulk information for extraneous purposes. This places our members in a most invidious position.”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

interaction with the official information statutes in this context has been problematic. Thus far in the chapter I have not directly addressed a recommendation to that inter-relationship.

- 7.16.2 Essentially a public register is an enactment which provides for access to personal information on a particular register. The information is usually also “official information”. Invariably public register provisions set out an entitlement to have access to information. Generally such provisions also describe the information to be made available. Sometimes a provision prescribes information that is not to be made available or place constraints upon subsequent use. Frequently, but not invariably, public register provisions outline the manner in which information is to be made available.
- 7.16.3 I believe that the inter-relationship between the Privacy Act and public register provisions, with the changes that I propose, is fairly satisfactory. The position is that a public register provision which expressly authorises or requires some action will prevail over the public register privacy principles and the information privacy principles. It will continue to do so under my proposals.
- 7.16.4 However, the position is made unsatisfactory by the fact that the official information statutes are not sufficiently clearly ousted from application to public registers. The intrusion of those statutes into matters which are specifically addressed by legislation in public register provisions and in the public register privacy principles is problematic, confusing and, in my view, quite unnecessary. The use of official information statutes by commercial interests to force the release of bulk information from registers makes the resolution of privacy concerns very difficult. I do not see the public interest as being served by bulk disclosures being forced on registrars and individuals in the name of “freedom of information”. There is, in my view, no public interest to be served by the disgorging of compulsorily obtained personal information to enable the preparation of marketing lists. Continuing “rulings” that such information must be handed over may bring the Official Information Act into disrepute.⁵³
- 7.16.5 I hesitate to prescribe precise solutions to the problem because they will affect not only the Privacy Act but also the official information statutes themselves. I am a firm supporter of open government and the aims of the Official Information Act but it seems to me that in this context something needs to be done to avoid the Official Information Act being used to upset any carefully crafted balance established in the public register provisions in particular statutes and under the public register privacy principles. The answer I suspect may be found in the interpretation of the savings provisions in the Official Information Act and the Local Government Official Information and Meetings Act or in their amendment.⁵⁴ A more limited proposal would make the official information statutes subject, in respect of public register provisions, to the proposed bulk release principle, thereby leaving untouched the position in respect of searches for individual records.



RECOMMENDATION 100

The official information statutes should be excluded from questions of release of personal information from public registers.

⁵³ In some cases the ruling may merely be the opinion of the Ombudsman that the official information legislation does not apply but that in his opinion the Act governing the register can be interpreted as requiring the bulk disclosure of the data.

⁵⁴ See, in particular, Official Information Act 1982, section 52(3)(b)(ii) and Local Government Official Information and Meetings Act 1987, section 44(2)(b)(ii).

“WCC believes that it cannot use the IPPs or PRPPs to address the concerns individuals have about the lack of control on the use and disclosure of personal information on public registers because LGOIMA and the legislation which sets up the public register over-rides the Privacy Act in most cases.”

- WELLINGTON CITY

COUNCIL, SUBMISSION T6