



Privacy Commissioner
Te Mana Matapono Matatapu

DP 1

REVIEW OF THE PRIVACY ACT 1993
DISCUSSION PAPER No. 1
STRUCTURE AND SCOPE

The Privacy Commissioner is reviewing the operation of the Privacy Act under section 26 of the Act. The Commissioner will consider whether any amendments to the Act are necessary or desirable and will report his findings to the Minister of Justice.

This paper is one in a series which will cover the entire scope of the Act and highlight some issues. To find out which other discussion papers have been released, and to obtain copies of them, contact the Commissioner's office. Copies of the discussion papers will also be available through the Commissioner's web site.

The Privacy Commissioner welcomes comments on this paper and seeks responses to any specific questions raised. Submissions should be made in writing and be forwarded to the Commissioner's office by post or email no later than ~~31 August 1997~~ **20 October 1997** (deadline extended).

The Commissioner will hold a series of consultation meetings in the main centres and some regional cities later in the year. If you would like to be invited to a consultation meeting please indicate this with your written submission.

Contact details for consultation

Privacy Act Review 1997
Office of the Privacy Commissioner
P O Box 10-094
Wellington

fax: 04-474-7595 privacy hotline: 0800-803-909 email: privacy@actrix.gen.nz

For general enquiries about the review please speak to the Enquiries Officers at the freephone number. If you have a more detailed enquiry concerning your submission or the review process please speak to the Codes and Legislation Officer at 04-474 7597.

Background information on the Privacy Act is available on the Internet at:
<http://www.knowledge-basket.co.nz/privacy/welcome.htm>

ISBN 0-478-10356-5

INTRODUCTION

This paper traverses several parts of the Privacy Act which bear upon its general structure and scope.

The discussion paper primarily covers:

- Part I of the Act: Preliminary provisions (sections 2-5);
- Part III of the Act: Privacy Commissioner (sections 12-26);
- Part XII of the Act: Miscellaneous provisions (sections 115-133).

The paper also canvasses the following provisions which link into discussion of structure and scope of the Act:

- section 1: Short title and commencement;
- section 56: Exemption for personal information relating to domestic affairs;
- section 57: Exemption relating to intelligence organisations;
- first schedule: Provisions applying respect of Commissioner.

Within each of the Parts of the Act under review there are a number of important sections. Some issues have been highlighted for discussion. Please feel free to offer comment relating to the operation of any of the provisions within these Parts of the Act regardless of whether they are specifically noted in the discussion paper. Some of the questions that have been posed in this paper have been suggested to the Privacy Commissioner by people in government, business and the public. The questions do not necessarily mean that the Commissioner considers that the present provisions are unsatisfactory.

Q. At the end of parts of the discussion specific questions, set out in boxes, are posed. These are to prompt responses - but comments are also sought on any other aspect of the sections under review.

PART I OF THE ACT: PRELIMINARY PROVISIONS

Part I sets out certain "preliminary provisions". In some respects the provisions provide the rules by which other provisions in the Act are to be understood. Section 2 (interpretation) defines terms used elsewhere in the Act. The definition of "agency", for instance, largely determines the scope of the Act's application.

Section 2: Interpretation

Section 2 is the key provision in the Privacy Act which assists in interpreting, and applying, all the other provisions in the Act. The section sets out a series of definitions which are used to give a standard meaning to words or phrases that occur frequently in the Act.

A good set of definitions is important to the effective operation of the Privacy Act. If terms are not well understood difficulties of interpretation and application will arise.

Q1. Are you aware of any particular definitions giving difficulty? If so, which ones? Why?

Difficulties may also arise if complex terms are left undefined. On the other hand, if terms are well understood, to include a special definition might cause, rather than resolve, difficulties.

People have suggested that the term "assigned" in information privacy principle 12 causes difficulty. This will be taken up in more detail in Discussion Paper No 2. However, the Commissioner is keen to hear from people as to whether this or any other term, currently undefined, should be given a special definition.

Q2. Are there any other terms which occur frequently in the Privacy Act that should be defined so as to give them a standard meaning? Which ones?

Feel free to answer question 2 even if you cannot suggest a suitable definition.

Section 2 is not the only place in the Act where terms are defined. Other definitions appear in sections 29 ("evaluative material"), 58 ("public register" and related terms), 66 ("interference with the privacy of an individual"), 97 ("information matching programme and related terms") and 110 ("law enforcement information" and related terms). Some of these definitions are referred to in section 2 (e.g. "information matching programme" and "public register").

The Law Commission considers that scattered definitions can sometimes obstruct a comprehensive understanding of an Act.¹ It has suggested that definitions are therefore best collected in one place, usually in alphabetical order early in the Act, but if there are many definitions, in a dictionary of definitions can be placed in a schedule at the back of legislation with a provision or note early in the Act informing the user where the definitions can be found.

¹ Law Commission, *Legislation Manual: Structure and Style*, 1996, paragraph 102.

Q3. Have the scattered definitions in the Privacy Act made it more difficult for you to use?

Most of the scattered definitions in the Act are collected together in places other than section 2 because the terms defined are only used in one Part or section of the Act. It may be that this is the most convenient place to locate such definitions

Specific definitions in section 2

Many of the definitions in section 2 are unremarkable and appear to have worked satisfactorily. The definitions noted below are those where an issue has been identified.

Be aware that some of the definitions (such as "document") have been derived from identical sections in the Official Information Acts.² Where that is the case there may be a need for consistency between the three Acts. Departure from existing definitions may lose the benefit of case law developed since 1982. On the other hand, a good case for amendment of any such terms may indicate that consideration should be given to amending the same definition in the Official Information Acts.

Agency

The definition of "agency" is particularly important as the information privacy principles are all expressed to apply to agencies. The definition starts out all-encompassing (a person or body of persons whether corporate or unincorporated and whether in the public sector or the private sector) but follows with a series of 13 exceptions. Accordingly, the exceptions are particularly important since they determine the overall scope of the Act.

Broad coverage is a prime feature of the New Zealand Privacy Act. Its seamless application to both public and private sectors means that most privacy issues are able to be reached by the Privacy Act. It also means that the legislation is little affected by demarcation disputes which accompany more narrowly based laws.

In reviewing the definition of "agency", consideration is really being given to whether the coverage of the Privacy Act should be narrowed (by creating new exceptions) or broadened (by narrowing or eliminating existing exceptions).

Q4. Should any new exceptions to the definition of "agency" be created? If so, which agencies should be exempted?

Q5. Should any of the existing exceptions to the term "agency" be repealed or amended? If so, which ones? Why?

Note that by being exempted from the definition of "agency" the relevant bodies are placed completely outside the privacy principles. It may be possible to avoid this by providing *partial* exemption. An example is found in section 57 (discussed below)

² Official Information Act 1982 and Local Government Official Information and Meetings Act 1987.

where intelligence organisations remain “agencies” but have a special exemption from certain of the principles. Some may see this as a better privacy protection than total exemption: a kind of “half-way house”.

Q6. Should any existing exceptions to the definition of “agency” be replaced with a partial exemption?

Several of the exceptions are included for what might be termed “constitutional” grounds. It might be seen as inhibiting to democratic processes to have members of Parliament in their official capacities subject to constraints as to how they use personal information and to make them subject to a complaints mechanism. The Bill of Rights Act 1688 also limits questioning of the proceedings of Parliament. Accordingly, MPs are exempted. For a related reason exemptions are provided for the House of Representatives, the Parliamentary Service Commission and, to a limited extent, to the Parliamentary Service.

A second set of exemptions are related to bodies carrying out judicial functions. Privacy issues do arise with courts and tribunals but such bodies have powers to regulate their procedure and attempt to deal with privacy issues through such mechanisms such as closed hearings and suppression orders and procedures for access to files. The next group of exemptions relate to Royal Commissions and related bodies such as commissions of inquiry. One complaint to the Commissioner has concerned a “University Visitor” which is a commission of inquiry.

Q7. Is there a case to revisit the exemptions granted to parliamentary agencies, judicial bodies or commissions of inquiry? If so, why?

The final exception relates to any news medium in relation to its news activities. The exception reflects the sensitivities with the competing public interests and the “freedom of the press”. Internationally, intrusions on privacy by the news media are widely discussed, particularly in Britain where a particular problem is perceived. One feature which points towards the desirability of an exception for the news media is that the privacy principles might not be very well adapted to the privacy issues encountered in relation to the news media. To be effective and appropriate they might need significant change. In this context, for example, the Broadcasting Standards Authority, which provides remedies for breach of privacy by broadcast media, has developed a set of privacy principles which follow an entirely different structure from the information privacy principles.

Q8. Should the current exemption for the news media be revisited?

Individual

The definition of “individual” excludes artificial entities, such as companies, and deceased people. These limitations may be thought to contribute to the straightforward operation of the Act since it avoids issues or interests which are on the fringe of true privacy concerns. Companies have an interest in controlling information about themselves but this may be more appropriately thought of as “commercial confidentiality” than privacy. Similarly, controlling information about dead people is of far less importance than protecting the privacy of the living.

On the other hand, excluding artificial entities and deceased persons from the definition of "individual", may make it difficult to address some issues such as:

- the privacy of the proprietor of the "one person company";
- the privacy of deceased persons and to a degree their families. The Privacy Act does acknowledge privacy interests of deceased persons in relation to the withholding of information pursuant to section 29(1)(a) and in relation to health information (section 46(6)).

Q9. Is any change to the definition of "individual" warranted? Should the current approach to information about deceased people be revisited?

Publicly available publication

"Publicly available publication" means a "magazine, book, newspaper, or other publication that is or will be generally available to members of the public; and includes a public register". This term is used in the exceptions to some of the privacy principles. For instance, information may be used or disclosed without restriction under principles 10 and 11 so long as the information comes from a publicly available publication. This exception contributes to the workability of the Privacy Act since it will be difficult to apply privacy principles to publications where there is, by definition, no control over how they are used and disclosed because of their "public availability".

There may be some difficulty in applying the concept of "publicly available publication" to less traditional non-printed or published media. Whether something is a "publication" that "is or will be generally available to members of the public" is not always clear. The Act deems public registers to be included in the definition but there is less certainty with regard to such materials as:

- statutory registers that are not "public registers" listed in Schedule 2 of the Act;
- official reports to which the public is entitled but which have not been published;
- material made available on an Internet web site but not otherwise published.

There may be a case to broaden the definition, to cover modern electronic publishing, or to narrow it, to ensure that the exceptions to the principles are not available in inappropriate circumstances to the detriment of privacy. Perhaps it may be best to stay with essentially the same definition but to clarify it in terms of any particular category of publication.

Q10. How broad should the concept of "publicly available publication" be? Should the present definition be broadened or narrowed? Should it be clarified in its application to any class of publication? If so, which classes?

Sections 3 and 4

Section 3 sets out the circumstances where information is deemed to be held by an agency. It makes a distinction between official and private capacities. Section 4 provides that for the purposes of the Act agencies are responsible for the actions of, or information disclosed to, their employees. Similarly section 126 provides that for the purposes of the Act an employee's actions are generally to be treated as the employer's, whether or not the latter knew or approved of them. A Law Society

working group has expressed concern that the inter-relationship between these three provisions is not always clear and suggests that the provisions may benefit from further clarification.

Q11. Have sections 3 and 4 worked satisfactorily in operation? What particular difficulties have been encountered? How might the sections be improved?

PART III OF THE ACT: PRIVACY COMMISSIONER

Part III of the Act establishes a Privacy Commissioner and sets out many of his functions, powers and organisational provisions.

Functions

Section 13 which sets out the general functions of the Commissioner. It is important for a Commissioner with a remit as a statutory guardian for privacy to have sufficiently broad functions. The general functions seem adequate when compared with the typical functions conferred on Commissioners in Australia and Canada.

Some of the Commissioner's existing functions have not been exercised in the last four years because they have not been needed yet, have not been priorities for the Commissioner, or because current funding does not enable the Commissioner to undertake them. For example, the Commissioner has not undertaken to maintain and publish directories of personal information under sections 13(1)(d) and 21 because it has not been a priority and because the likely cost of such an undertaking could not presently be met. The Commissioner is authorised to undertake audits of agencies pursuant to section 13(1)(b) but has not done so partly because of the resources that would be involved. At present, the Commissioner could only contemplate undertaking auditing functions if the costs were to borne by the agencies being audited. As the agencies must voluntarily agree to be audited this option has not yet been seriously explored.

Q12. Should any new functions be conferred on the Privacy Commissioner in section 13? Should any existing ones be changed?

Two further functions have so far been suggested for the Commissioner.

The first relates to the Commissioner's role in respect of reviewing "reasonable charges" for giving access to personal information held the private sector. The Commissioner handles complaints in respect of such charges³ and may by code of practice deal with charging.⁴ However, complaints only arise on a specific set of facts and codes are generally issued only in relation to a particular sector. Some have therefore suggested a role for the Commissioner to set charging principles to offer clearer general guidelines. This issue will be taken up further in Discussion Paper 3 but initial reactions are welcomed.

Q13. Should the Commissioner be empowered to issue guidelines on charging for access to information?

A further function has been suggested in relation to transborder data flows. This would relate to the export of personal information from New Zealand to other jurisdictions. Internationally a lot of attention has been given to this issue. The issue was central to the OECD guidelines on which the Privacy Act is based. A recent

³ See section 78 of the Act.

⁴ See section 46(4) of the Act.

European Union Directive on Data Protection⁵ will oblige EU states to place controls on the export of data to any country which does not have "adequate" privacy laws. Data export provisions have been included in most European laws. Others will be modified to meet the EU directive. Controls also appear in the Hong Kong law.

One suggestion has been to empower the Commissioner to act in particular circumstances to prohibit the export of data or to allow its export only on terms set out in the Act. One such circumstance might be where it was believed that data was being routed through New Zealand and re-exported elsewhere so as to circumvent EU controls (to avoid New Zealand's laws being seen as having a "loophole"). Another might be where a sensitive category of data is proposed to be transferred to a jurisdiction having no privacy laws. It is proposed to develop this issue further in a later discussion paper. Initial comments are welcomed.

Q14. Should the Commissioner have a function with respect to information export/transborder data flows? If so, what considerations should be taken into account in preparing any such provision?

There are a variety of other sections in Part III of the Act. Some of these are quite important but, as they only apply to the Commissioner, other people will be unable to relate any experience in relation to them. However, the section concerning privacy officers affects every agency in the country and therefore the Privacy Commissioner is particularly keen to hear views as to its operation.

Privacy officers

Section 23 provides that each agency has the responsibility to ensure that there is a privacy officer. The section explains what the privacy officer's responsibilities are. It is suggested that the section has been quite successful as a statutory mechanism to introduce the law to a variety of agencies in the public and private sectors and to ease compliance. A heavy handed approach is not taken and there is no specific offence of failing to appoint a privacy officer. Many businesses have seen the benefit of giving the responsibilities of a privacy officer to an appropriate employee and giving that the person the authority, support and training that they need.

A variety of approaches have been taken to suit the style of particular agencies. Some have appointed a very senior executive to the post who has, after developing suitable policies delegated some of the functions. Others have devolved functions to 3 or 4 district or assistant privacy officers.

The Commissioner believes that there is value in the position of privacy officer and that it has worked relatively well. However, he is interested to know whether others also take this view. A number of agencies have failed to appoint privacy officers or, as a holder of the responsibility has left, have failed to confer the functions on another employee. It is perceived that agencies with privacy officers (and particularly with well trained privacy officers) seem to have less difficulty with statutory compliance than those without.

⁵ Directive on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data, European Union, 24 October 1995.

Q15. Has the provision relating to privacy officers worked well in operation? Can it be enhanced? Should section 23 provide a sanction for failing to have a privacy officer?

PART XII: MISCELLANEOUS PROVISIONS

Part XII of the Act, which encompasses sections 115 to 133, contain an assortment of technical and substantive provisions. Given their wide variety, and technical nature, most will not be mentioned in this paper although submissions on any section are welcomed.

Sections 124 and 125, which run to almost two pages of the statute, concern delegation of powers by local authorities and by offices of local authority. The Commissioner would be interested in comments, particularly from local authorities, as to how they have found these provisions in operation and whether they would prefer to do without them or to have them located in the Local Government Act.

Q16. Are sections 124 and 125 really necessary? Would local authorities find it more convenient to have delegation powers located in the Local Government Act rather than the Privacy Act?

Offences

Section 127 is the offence provision. Unlike some overseas privacy laws, there are very few offences in the Privacy Act. For example, it is not an offence to breach an information privacy principle. Rather, the Act emphasises civil remedies. If an agency breaches a privacy principle, and an individual has been harmed as a result, the Act can provide a resolution to an individual's complaint, and, if necessary, to compensate that individual. That approach is preferred to the criminal law approach, which would seek to punish an agency in such circumstances. Both approaches are directed towards preventing a repetition of the action but the civil law approach is seen as less "heavy handed" and ensures that the individual, who should be at the centre of any privacy process, is given redress if possible.

It is possible that some suitably crafted offences may nonetheless make the legislation more effective in certain aspects. If new offences were to be included, care would need to be taken to decide where the existing civil law approach is solely appropriate and where the criminal law could provide a supplement. It is suggested that any new offences should be crafted to apply:

- to the exceptional cases since, by and large, the privacy principles should be able to do the job they are given;
- be directed at persons who by their wilful acts put otherwise innocent agencies in breach of the privacy principles or otherwise undermine the proper operation of the Act.

Q17. Is it appropriate to consider introducing new offence provisions into an Act largely based on civil remedies? If so, what general approach should be taken towards suggestions to include new offence provisions?

One new offence which might be considered would concern the actions of a person who knowingly makes a request for access to, or correction of, personal information under false pretences. This would reflect the fact that the Privacy Act has obliged agencies in the private sector to open up their files to individuals where previously they may have kept them far more securely closed to outsiders. In such circumstances the

agency is put at risk, as is the privacy of the individual concerned, if a person impersonates the individual entitled to have access or misrepresents the position by claiming to have authorisation to have access to information. Under the present approach the Privacy Act in such circumstances the only remedy for the aggrieved individual is take a complaint against the agency. At best, the individual may obtain redress from the duped agency for disclosure of information or a failure to take reasonable security safeguards and at worst will obtain no redress. There will be no recourse under the Privacy Act against the individual who has deliberately misrepresented the position. In some cases the individual who has misrepresented the position can even take advantage of the domestic affairs exemption in section 56 of the Act if they have can show that they collected the information in connection with their personal, family or household affairs.

This issue also exists in other jurisdictions. The New South Wales Privacy Committee has, for example, recommended the creation of such an offence. In the UK an offence to achieve such a result was enacted in the Criminal Justice and Public Order Act 1994. Such a provision has existed for some time in the Privacy Act in the USA.⁶

Q18. Should there be an offence created where a person intentionally misleads an agency into giving access to information under principle 6, or correction of information under principle 7, by impersonating the individual concerned or misrepresenting authorisation from that person?

A second possible offence has been suggested in relation to destroying information to which a person is entitled to have access in order to deny that person their rights. An example is the deliberate destruction of documents after an access request has already been received. A variation on this would be to falsify a document so as to purport to give access to information whereas access is actually being denied. It might be argued that these could possibly breach information privacy principle 6 in any case and therefore the civil remedies may be available. Whether or not that is correct, it has been suggested that such actions are of an "immoral" type going beyond the normal breaches of information privacy principle 6 (which do not necessarily carry any moral overtones) and therefore they might appropriately be criminalised. Even if a remedy is available to the individual, it is suggested that it might be appropriate to punish the person or agency which has knowingly destroyed the information or doctored the documents as the actions seriously undermine the objectives of the Act.

Q19. Should there be an offence of knowingly destroying information to which a person is entitled to have access in order to deny the person that right?

Finally, it has also been suggested that an offence provision should be created in relation to hacking into a computer in order to obtain access to personal information or to manipulate it. Many commentators have suggested that New Zealand's computer crimes law are inadequate and official reports have suggested the creation of new offences. However, the issue in this context would be whether the Privacy Act is an appropriate vehicle to introduce such offences.

⁶ The Privacy Act 1974 (USA) provides that any person who knowingly and wilfully requests or obtains any record concerning an individual from an agency under false pretences shall be guilty of a misdemeanour: penalty \$5000 fine.

Q20. Should the Privacy Act include any computer crimes, such as hacking into a computer in order to obtain access to personal information or to manipulate it?

OTHER PROVISIONS

The final part of this paper touches upon some provisions which sit better with this "structure and scope" discussion paper than any other. Feel free to offer any observations on sections 1, 56 and 57, and the First Schedule, even if the issue is not raised in the discussion paper.

Section 1

Section 1 sets out the short title of the Act ("Privacy Act 1993") and the commencement date. Unremarkable in itself, it follows a more interesting *long* title. The Law Commission has suggested that purpose provisions help users of legislation to understand the particular Act or part of an Act to which the provisions relate. The Privacy Act has no "purpose provision" but the long title possibly fulfils a similar function. The long title, explains, for instance, that the Act is to promote and to protect individual privacy" and that it is to do so "in general accordance with" certain OECD guidelines.

Q21. Are any changes to the long title desirable?

Sections 56 and 57

Sections 56 and 57 are partial exemptions from the application of some of the information privacy principles. The effect of any change to sections 56 and 57 may be felt in several ways. If the existing exemptions are broadened then it means that the application of the privacy principles will be narrowed and arguably the protection of privacy diminished. If the exemptions are narrowed then the application of the principles will be enlarged and arguably the protection of privacy enhanced. However, both exemptions are there for a reason. If either exemption is narrowed it may be that some difficulties are caused for the relevant agencies or in respect of the interests for which the exemptions have been created.

Section 56

Section 56 creates an exemption in respect of personal information collected or held by an agency that is an individual where the information is collected or held by that individual "solely or principally for the purposes of, or in connection, with that individual's personal, family, or household affairs."

This is based upon an existing exemption in the Data Protection Act 1984 (UK). The Hong Kong privacy law, which has a similar coverage and approach to the New Zealand Act, has adopted a slightly broader exemption. In addition to "personal, family, or household affairs" the Hong Kong exempts personal data held by an individual for "recreational purposes".⁷

Some problems have been encountered where family members engage in misleading conduct. The most common example is where an estranged spouse misrepresents to an agency that he or she is authorised to have access to personal information about the other spouse. Some individuals impersonate other family members in relation to

⁷ Personal Data (Privacy) Ordinance 1995, section 52.

agencies. It appears that even in such circumstances individuals may be able to rely upon the exemption. Questions have been raised as to whether this is appropriate.

Q22. Should the domestic affairs exemption be amended? For instance, should it be broadened along the lines of the Hong Kong law? Is it appropriate to prevent individuals relying upon the exemption where they have deliberately misled an agency so as to improperly procure the disclosure or alteration of information?

Section 57

Section 57 provides that nothing in principles 1-5 or principles 8-11 applies in relation to information collected, obtained, held, used, or disclosed to, or disclosed to an "intelligence organisation" (that is, the New Zealand Security Intelligence Service and the Government Communications Security Bureau). Therefore, only principles 6 and 7 (access and correction) and 12 (unique identifiers) apply to the SIS and GCSB. Access and correction rights are less useful than might be expected since requests to intelligence organisations for access to information may sometimes be met by a "neither confirm or deny" response.⁸

It is timely to consider whether further information privacy principles should be applied to intelligence organisations. There may be a case for applying some of the principles, but not all of them, taking into account security needs. The Commissioner considered this matter when he examined the Intelligence And Security Agencies Bill and concluded that:

- information privacy principles provide a sound basis for fair information handling practices and have clear relevance to intelligence organisations; and
- principles 1, 5, 8 and 9 in particular ought to be applied to intelligence organisations.

The Commissioner focused upon those principles as they take account of the purposes of the agencies concerned, apply standards that are reasonable in the circumstances, and would not need to be amended to establish any national security exceptions.

Q23. Should the exemption for intelligence organisations should be narrowed or left as it is? If it should be narrowed, which additional principles should be applied to intelligence organisations?

First Schedule

The First Schedule sets out a number of unremarkable administrative provisions allowing the Privacy Commissioner to employ experts and staff, make certain payments, deal with the Commissioner's funds and bank accounts, etc.

One provision has been raised for reconsideration. Clause 2(3) provides that the number of staff that may be appointed, whether generally or in respect of any specified duties or class of duties, is from time to time to be determined by the responsible Minister. The question has been raised as to whether such a broad control as this has any merit in terms of financial accountability and whether it may be seen as

⁸ See Privacy Act, section 32.

encroaching upon the independence of a Commissioner. It is noted that a similar provision was recently deleted from section 28 of the Ombudsman Act.⁹

Q.24 Should the responsible Minister have the power to determine the number of the Commissioner's staff either generally or in respect of any specified duties or class of duties?

In this brief discussion paper it has not been possible to canvas the full range of issues bearing upon the structure of the Privacy Act. The Commissioner welcomes any other views and will be considering other matters not specifically mentioned. Some of these may be mentioned in later discussion papers.

Among the sort of issues that the Commissioner will consider are:

- whether any provisions should be reordered or redrafted to aid effective understanding and decision making;
- whether existing marginal notes to the Act are as helpful as they might be (several are not, see for example section 27);
- whether the general provisions of the Act, such as the privacy principle, effectively relate to the particular parts of the Act, such as those on information matching and public registers;
- whether any structural changes are desirable to achieve an appropriate balance between flexibility, certainty and clarity;
- the relationship between the key entities referred to in the Act: the individual, agencies, Commissioner and Complaints Review Tribunal.

This is merely a small taste of the many issues the Commissioner will wish to consider. Any suggestions are welcomed.

The Privacy Commissioner may include in his final report a list of submissions received. He may also refer to submissions in the text of his report. If you want your submission or any part of it treated confidentially, or do not want it used in this way, please indicate this clearly. The Commissioner is subject to the Official Information Act. Copies of submissions may therefore be released on request. Any request for the withholding of information on the grounds of confidentiality or for any other reason will be determined in accordance with that Act and section 116 of the Privacy Act.

act-revi/discuss/discppr1

⁹ Refer Ombudsman Amendment Act 1996.