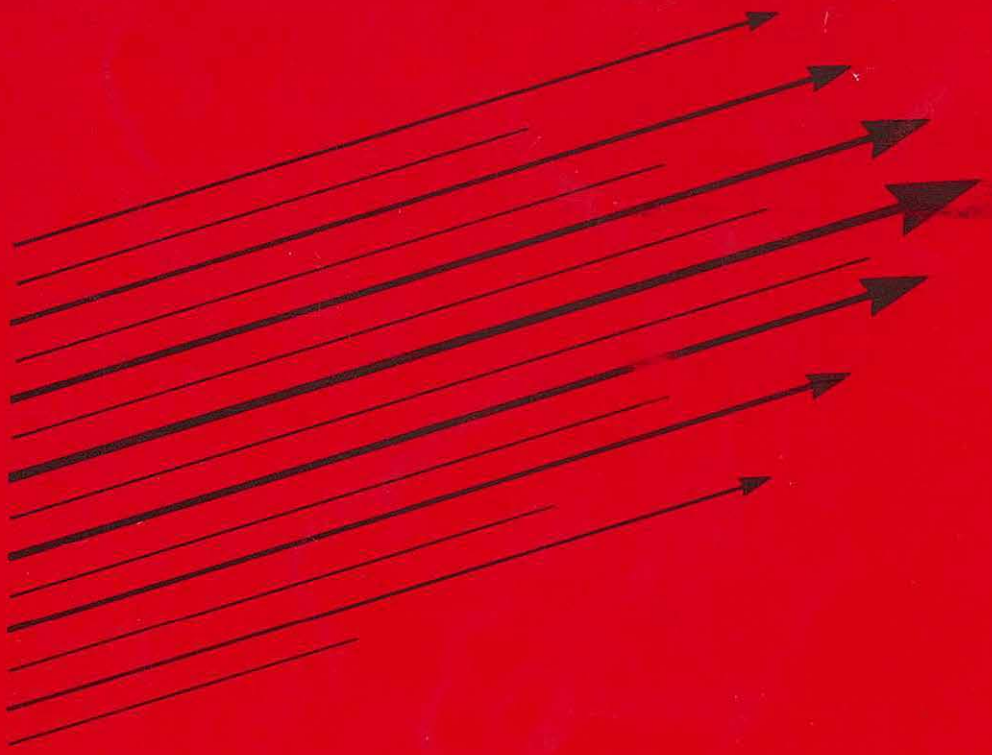
THE
INFORMATION
AUTHORITY



PERSONAL INFORMATION AND THE OFFICIAL INFORMATION ACT: RECOMMENDATIONS FOR REFORM

THE INFORMATION AUTHORITY

PERSONAL INFORMATION AND THE OFFICIAL INFORMATION ACT: RECOMMENDATIONS FOR REFORM

Wellington
New Zealand 1987

Published by

THE INFORMATION AUTHORITY

P O BOX 10-351

WELLINGTON

CHAPMAN TRIPP
SHEFFIELD YOUNG

NEW ZEALAND 1987

ISBN. 0-473-00460-7

Copies available from Government Bookshops, Private Bag, Auckland, Hamilton, Wellington, Christchurch, Dunedin. Cost $8.25 including GST.

CONTENTS

FOREWORD

Unqualified approval is rare where public affairs are concerned, but it certainly appears to attach to the phrase 'Open Government' which has come to be associated with the Official Information Act, emphasizing that Act as a means to bring about the release of official information. It is an appropriate and desirable description of a reform designed to bring one aspect of the conduct of public affairs out from under the shadows of the Official Secrets Act.

But, as a reading of the Official Information Act duly reveals, it is not enough to call attention only to the openness and release capability of the Act. To do so is to overlook that important part of official information which deals with personal information. How shall information which identifies persons and individuals be protected when it is in official hands, in the interests of the privacy people are entitled to expect?

In one place or another, scattered through our Public Acts, are references to the collection and use of personal information, which may have been elicited voluntarily or compulsorily. This is a growth industry in the circumstances that the expanding responsibilities of government require to be served, and the technical ability to handle information is increasingly facilitated by electronic devices.

The protection of privacy is a matter of serious political, even constitutional, importance in the establishment of relationships between the individual and the State. The text of the following report examines the extent and significance of means to deal with this question as it relates to official information. Ways to effect reform are set out following lines of action already employed in the Official Information Act and, more recently, in its important Amendment Act.

The method is to extend the legislative basis, codifying the relevant entitlements and responsibilities to form a comprehensive regime for official information matters. The clauses so spelt out exercise a general suzerainty over the information processes of government. By drawing information matters away from separate Public Acts into the Official Information Act, a single comprehensive instrument to deal with information privacy is established. The general approach taken in the Act, of weighing the protection of information against the public interest which may lie in releasing it, is here sustained in a proposed additional section 9A.

It should be recognized that this new mode of dealing with personal information will modify its collection and use and, in calling for justification for particular cases, will desirably constrain the conduct of public affairs. The further step, however, which might have been taken, the introduction of a separate Privacy Act, awaits a yet more comprehensive reform exercise.

You are invited to send comments on the issues raised in this booklet to -

The Chief Executive Officer
Information Authority
P O Box 10351
WELLINGTON

by 31 July 1987

Alan Danks K.B.E.
CHAIRMAN

Chapter One

BACKGROUND TO THE RECOMMENDATIONS FOR REFORM

INTRODUCTION

The Official Information Act 1982 (OIA) established the principle that information held by government agencies covered by the Act should be made available to the public unless there was good reason for withholding it. Amongst those reasons is the protection of privacy of natural persons and the confidentiality of competitive commercial information, where it could reasonably be expected that harm would result from release. Section 4 of the OIA, which states the purposes of the Act, while providing for availability of information and the resulting accountability of Ministers and officials, also requires that information be protected "to the extent consistent with the public interest and the preservation of personal privacy.". The Act further recognised the dangers for individuals in the assembly of information and reflected wider concerns in the community regarding the development of information technology. It required the Information Authority (section 39), to examine the fairness and reasonableness of department's and organisation's existing and proposed powers that require persons to supply information about themselves; and to decide whether the use made of the information was proper where it was being used for a purpose other than that for which it was obtained.

Greater controls on the collection, use and security of personal information now call for attention. In 1985 the Information Authority published a discussion booklet entitled "Personal Information and the Official Information Act: An Examination of the Issues". Its purpose was to raise issues about the collection, use and storage of personal information by Government agencies - issues that arise primarily from the concepts of information privacy. The booklet promulgated certain principles (listed on pages 12 to 14) and was sent to organisations likely to have an interest in such matters, as well as to all departments and organisations covered by the OIA. The principles were generally agreed to by those who responded to the Authority's invitation to comment.

OTHER PUBLICATIONS

Just prior to the booklet being published the Human Rights Commission published 'Privacy Review", a discussion and resource paper (a substantial work) by Mr T J McBride, Senior Law Lecturer, Auckland University. Since then a NZ Computer Society and NZ Law Society report on data protection has been released and the Computer

Society has promulgated amongst its members a code of ethics in relation to security of information on electronic systems.

Both Government and the Opposition have spoken against the use of a general identification number for all New Zealanders, linking it to a potential invasion of privacy through possible computer matching. They saw this as enabling the compilation of extensive 'dossiers' on individuals, the use of which could be harmful to the people concerned. The issue of privacy was touched on by the Wanganui Privacy Commissioner in his Annual Report in relation to possible unauthorised use of the computer and also in general philosophical terms. There has also been continued discussion on privacy and information security through the media.

It is not the Authority's intention to repeat the more detailed content of its first discussion book. For those who are interested in reading it, copies are available from Government Bookshops, Private Bag (Auckland, Hamilton, Wellington, Christchurch or Dunedin), at a cost of $5.45 which includes GST. To assist the reader put the proposed collection and use legislation into context, however, we give a brief outline of the issues.

WHAT IS PERSONAL INFORMATION?

Any information held about an identifiable person is personal information. The definition in the OIA includes "legal" persons such as companies, trade unions, incorporated societies and other bodies of persons, whether corporate or unincorporate, as well as individuals or "natural" persons. The task of the Authority when considering "personal information" has, therefore, been wider than that of individual privacy - it has also covered information on legal persons, including commercial entities.

THE STATE'S NEED FOR PERSONAL INFORMATION

The state's need for personal information inevitably arises from the nature of the duties imposed upon a public agency. Sometimes it is required for positive results for the supplier (social welfare benefits), sometimes for a 'state interest' (customs and tax collections), and sometimes for statistical or research purposes. The more the public require the State to provide social services, or to intervene in some way in the economy, the more personal information it will need to carry out those functions efficiently and effectively. The wide range of present functions requires information from individuals about many aspects of their lives and from organisations about their business. The following are examples.

* If you want a medical benefit, or an Accident Compensation refund, or to take out a life insurance policy, it is reasonable to expect that a medical referee's report will be

needed.

* To ensure that homes for the elderly are up to standard and well run information must be supplied to the Health Department which licences and monitors them on behalf of the public.

* To enable better planning for our hospitals and health systems information is needed on patients from which statistics on health status and services can be compiled.

* To ensure duty is paid on imports and disease is not brought into the country, details of sea and air passengers' effects must be advised.

* Social welfare benefits and the assessment of tax liability both mean the production of extensive amounts of personal information.

* To check that all TV sets are legally licensed, sellers must advise the Post Office of all sales to enable owners who have not paid their license fees to be brought to account.

* A great deal of commercial information from companies is needed when the Commerce Commission is considering a merger or takeover application, or the Securities Commission is carrying out an investigation.

WHAT INFORMATION IS COLLECTED?

Departments and organisations were asked to advise the Authority of the personal information that they collected, the authority for and methods of collection, the use made of the information and how it was stored. To date we have been given details of 768 separate types of collection and told, in general terms, of at least another 700.

Of those 768 different collections:-

389 have a power of compulsion;
391 resulted in some benefit to the supplier through receipt of welfare payments, licences, loans etc;
78 covered commercial practices and operations;
92 related to taxation and economic matters;
108 were to do with employment and appointments (personnel matters);
104 were concerned with public health and safety;
76 related to registrations for a trade etc, and licensing;
695 were held in manual systems;
135 were held on electronic systems.

Some of the collections fit into more than one category,

e.g. commercial information for licensing purposes, that also gives a benefit to the supplier of the information, while some information is stored in both manual and electronic systems. In our previous booklet we listed examples of the powers requiring compulsory supply of personal information and this is repeated here for convenience. (See Appendix I)

INFORMATION TECHNOLOGY

The last decade has seen new information technology bring to New Zealand an ever-increasing capacity for handling information. Government departments and agencies have shared in the new processes which have been timely in view of the increasing State intervention on behalf of economic and social welfare. The gathering and processing of personal information as a result of this has been a growth industry in the last two decades and this is likely to continue.

LINKAGE

Until the age of the computer, with its potential to match and aggregate large amounts of data, the possibility of personal information held in one department easily being accessed by another was remote. Today it would be possible to assemble extensive profiles of individuals and corporate bodies and their activities which could be used, unbeknown to them, to their disadvantage. Such aggregation also increases the possibility of misuse of information because of the remoteness of the decision maker from the subject of the decision. The ability of computers to 'match' information allows the possibility of 'fishing expeditions' to check records for possible illegalities or fraud. This means there is an assumption that everyone is guilty until proven innocent, the reverse of our present law that presumes innocence until proven guilty. A US Department of Health, Education and Welfare Report July 1973, 'Records, Computers and the Rights of Citizens', said

> .."*public concern about such combinations of data through linkings and merger of files is well founded since any compilation of records from other records can involve crossing functional as well as geographic and organizational boundaries. When data from an administrative record, for example, become part of an intelligence dossier, neither the data subject nor the new holder knows what purpose the data may some day serve. Moreover, the investigator may believe that no detail is too small to put into dossier, while the subject, for his part, can never know when some piece of trivia will close a noose of circumstantial evidence around him.*"

Technology makes it important to establish criteria to control the

development of government systems that use personal information.

BALANCING PUBLIC AND PRIVATE INTERESTS

In its concluding chapter of the discussion booklet the Authority said -

> *"The legitimate needs of public institutions in acquiring personal information and the use to which this is put needs to be pitched against the legitimate concerns in restricting the use or dissemination of the information. A recognition of this is contained in a number of international declarations or significant overseas conventions. These are:-*
>
> * *the Universal Declaration of Human Rights 1948;*
> * *the UN Covenant on Civil and Political Rights 1966 (ratified by NZ in 1978);*
> * *OECD Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data (NZ is a signatory to these guidelines);*
> * *the Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, December 1982.*
>
> *The basic values which underpin privacy interests include individuality, personal autonomy, and fairness. These provide the basis for describing an interest of the person or organisation in controlling personal information so that it is not collected, or used by the record-keeper or another party in a way that is inimical to the subject. There is general agreement that the risk of misuse is increasing with the development of technology and the greater demand for information by the Government for planning, research and the implementation of the diverse functions now carried out by the State. The present safeguards and remedies available to meet these risks to information privacy are not adequate."*

COLLECTION AND USE PRINCIPLES

The Authority then presented for public discussion a number of principles to govern the collection and use of personal information. They had largely been distilled from overseas reports such as the Australian Law Reform Commission's report on Privacy, and the OECD guidelines on data protection.

THE PRINCIPLES

Collection:

The power of collection is considered to be fair and reasonable where it complies with the following:

1. *NECESSITY*
   Personal information is not collected unnecessarily.

2. *FAIR COLLECTION*
   Personal information is obtained and processed fairly and lawfully.

3. *INFORMING*
   The person that collects personal information takes reasonable steps to ensure that, before it is collected, or if that is not practicable, as soon as practicable after it is collected, the record-subject is told:-

   (a) the purpose for which the information is being collected, unless that purpose is obvious;
   (b) if the collection of the information is authorised or required by or under law - that the collection of the information is so authorised or required; and
   (c) in general terms of the record-keepers usual practices with respect to disclosure of personal information of the kind collected.

4. *PRECISE POWER*
   When exercising a statutory power of entry, the acts the official can perform, the question that s/he may ask once s/he has gained admission and the uses s/he may make of any information that s/he acquires following entry, is related to the purposes of the particular entry and is specified as precisely as possible.

5. *RELEVANCE*
   A person should not collect personal information that is inaccurate or having regard to the purpose of collection is irrelevant, out of date, incomplete or excessively personal.

6. *QUESTION*
   The relationship between the privilege against self-incrimination and an officials power to ask questions should be clarified in respect of each separate power, preferably by expressly affirming the privilege.

7. *OBJECTIVE BELIEF*
   The grounds for collection of personal information should be objective not subjective.

Use (Including Disclosure):

The use of personal information is proper where it complies with the following:

8. *RELEVANCE*
   It is used for a purpose to which it is relevant

9. *PURPOSE*
   It is used only for the purpose for which the information is collected, or a purpose incidental to or connected with that purpose unless:-
   (a) the record subject has consented to other use;
   (b) the person using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person; or
   (c) the use is required by or under law.

10. *ACCURACY*
    The person who uses personal information takes reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

11. *CONSENT*
    The record-keeper does not disclose the personal information about the subject to a third person unless:-
    (a) the record-subject has consented to the disclosure
    (b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or some other person; or
    (c) the disclosure is required by or under law.

12. *SECURITY*
    The record-keeper takes such steps as are in the circumstances reasonable, to ensure that personal information held by the record-keeper or under his control is securely stored and is not misused.

Access:

How persons may find out what Personal Information is held on them; and the steps necessary for information to be corrected.

13. *RIGHT OF ACCESS*
    Where a person has in his possession or under his control records of personal information the record-subject should have access to those records.

14. *POWER TO REQUEST CORRECTION*
A person who has in his possession or under his control a record of personal information about another person should correct it so far as it is inaccurate, or having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, misleading, out-of-date, incomplete or irrelevant.

15. *OPPORTUNITY TO KNOW OF INFORMATION HELD*
The subject should be informed of the existence of personal information held, particularly where this information is of a disparaging nature and is to be used in decision making.

16. *INTERMEDIARY ACCESS*
Where direct access is impracticable, or may be harmful to the subject, intermediary or third party access should be available.

.....

RESPONSE TO THE BOOKLET

The discussion booklet was distributed widely to the media, to interested groups, to Members of Parliament and to departments and organisations covered by the OIA. While most of the departments and organisations responded to the invitation to comment and acknowledged the importance and sensitivity of the issues raised we were disappointed that very little coverage was given by the media who evidentally did not see the importance of the proposals. Replies were also received from bodies such as the N Z Law Society and the N Z Computer Society. There was considerable support for the principles and most departments saw little or no difficulty in their implementation. Some suggestions for change were made, but these generally concerned a specific problem, mainly to do with intelligence and investigative questions of limited scope. The Authority has not been persuaded that the generality of the principles need change, but agrees that in certain instances there may need to be exceptions to the general rule. Where this is the case, the exceptions should be clearly stated, rather than a general principle be amended to a stage where it has little or no force.

Chapter Two

MEASURES FOR REFORM

IMPLEMENTATION OF THE PRINCIPLES

Considerable thought has been given to how the principles could best be implemented. Whatever is proposed must take into account the present legislative powers of collection and use as well as provide for compatibility with such powers in future legislation. It is not intended that the principles should supplant those powers, rather that they enhance them and set the boundaries and rules for their use.

First consideration was given to establishing the principles as guidelines to be followed by departments and organisations when developing legislation and implementing powers to collect and use personal information. But, like the Committee on Official Information (General Report, Page 6), the Authority did not think administrative directives to heads of departments and agencies would achieve the desired results, regardless of the goodwill towards the guidelines. Without the force of law, persons from whom sensitive information is being obtained would have limited confidence that the information would be handled with care and not, in their eyes, misused.

We next considered developing model clauses that might be used by departments when drafting or amending legislation that gave powers to collect personal information and bring it into line with the privacy principles. After considering the number of provisions involved, however, it was agreed that this would be too costly in time and resources; neither would it cover information that is not required by statutory powers.

It was decided that the only practical way to proceed and the one which would incur the least difficulty for departments and organisations, yet give credibility to the exercise for those required to provide the information, was to include general provisions within the OIA. We are, therefore, recommending amendments to the Act to govern the collection and use of personal information from both natural and legal persons. The present and future powers of collection in other legislation would remain, but their operation, in general, would be subject to the provisions in the OIA.

There may, however, be at least two particular types of statutory provision that will remain significant. The first is that provision which grants the power to compel the supply by an individual of particular information and where the need for collection is

justified within the statute. The other matter which should be dealt with specifically, if there is a power of compulsory acquisition of information, is self incrimination. A basic principle of law is that the prosecutor must establish guilt and individuals should not be subject to compulsion to provide evidence of their own guilt. In some circumstances, however, the law departs from that principle, e.g. on the basis there is no other good source of relevant information. Any departures should be justified and the matter should be clarified and specifically stated in any peice of legislation that requires disclosure of information that could lead to self incrimination.

To achieve the general regime discussed in the previous paragraphs we propose clause 23H, an 'applications' provision that would provide for the OIA to be read with the individual powers and control their implementation. Precedents for this type of provision are found in the Quebec, Ontario and USA privacy legislation, as well as Clause 53 of the Local Government Official Information and Meetings Act. The relationship between existing powers of collection and use and the new clauses 23A to 23G here proposed, calls for careful examination in the light of clause 23H. Difficulties foreseen should be brought to the Authority's attention.

Clause 23H at present provides two avenues whereby other legislation may be excepted from the proposed collection and use rules in clauses 23A to 23G. We discuss the issues that give rise to these exemptions in the next paragraph on the scope of the legislation.

THE SCOPE OF THE LEGISLATION

The Authority's brief lies with that information collected by Departments and organisations covered by the OIA, essentially the public sector, and covers information held in both electronic and manual systems. We believe that it would also be appropriate for the proposals to be included in any local government official information legislation. The proposed Local Government Official Information and Meetings Act is, in essence, the OIA adapted for local government information.

In the general case the legislation would cover all official and potential official information. There may, however, be particular information to which it would not be appropriate to apply the proposed legislation. This could be an Act where there is already a detailed code or regime for collection and use, such as the IRD Act, or where there are specific controls on usage that are narrower than the proposed general provisions, or where legislation controls the type of questions that can be asked in a certain situation, or specifies that certain information must be released in a particular circumstance.

One area of collection and use that needs special consideration is that of information for and in intelligence systems developed for detection of crimes. By their very nature such systems are collectors of some information that may be hearsay or circumstantial, and in fact untrue. Checking the accuracy of such information can be difficult and costly, and frequently, as with drug offenders, to check with the subject would be to negate the whole purpose of the collection. Operators of such systems usually have their own internal rules for deciding what information should be included or discarded, when the system should be audited and how, and who may have access to the system, both for inputting and outputting information.

There will also be occasions when the departments and organisations acquire information for possible prosecution procedures. Does there need to be a general exemption for this information or should there be the ability to review a decision not to advise the subject of collection? Proposed clause 23B, which requires information to be collected directly from the subject, does give exemptions to the requirement. One of these is "where such collection would prejudice the purpose of the collection." Under this section a decision not to tell the subject of the collection could, if the subject becomes aware of it, be complained of. The Authority suggests that this provides a better balance between the interests of the State and of the subject, than to exempt such information altogether from the possibility of a review of the agencies' decisions not to advise of collection. Comments on these issues will be welcome.

RESOLUTION OF DISPUTES

An important part of the operations of the OIA concerns the review of decisions about the protection or release of information. A party questioning a decision by a department or organisation may appeal to the Ombudsman.

There seems no good reason why this review procedure should not apply to the extended provisions of the OIA here proposed. No doubt decisions affecting personal information will come to be called in question, and a due process to care for this should be in place. The informality which marks the means of seeking recourse through the Ombudsman is highly desirable and should embrace these new provisions.

It should be recognised, however, that this review system operates only in response to individual requests arising out of particular circumstances. A larger view of the responsibilities of review, in the different sense of a systematic and generalised study of information matters, requires a different approach and different means. The Information Authority is disestablished in June 1988 and its general functions of assessment and recommendation for modification will lapse. The extensions to the OIA here proposed

add to the need for some provision to be made in due course for a general review function to be exercised.

WHY NOT A SEPARATE PRIVACY ACT?

The long title of the Official Information Act states that it is "an Act to make official information more freely available, to provide for proper access by each person to official information relating to that person, to protect official information to the extent consistent with the public interest and the preservation of personal privacy, to establish procedures for the achievement of those purposes, and to repeal the Official Secrets Act 1951".

With the inclusion of the reference to personal privacy in the title, together with the access procedures in Part IV of the OIA and the requirement in section 39 to review procedures for the collection and use of personal information, the Authority believes that separate legislation would not be appropriate. It is more helpful to have the umbrella legislation establishing a general official information regime in one statute, as it should prove easier to understand and administer, and should ensure harmony between the concept of a general access and the need to protect sensitive personal information. (See Section 4 of the OIA.) There is also a need to eliminate conflict between the reasons for protection of information and the exemptions for other use. Where the rules are in one Act, conflict is less likely to occur. Finally, the access procedures that persons may use to check if information held about them is accurate and if not may require correction, (which are an essential part of any privacy legislation), are already in Part IV of the OIA. The rules governing collection and use of personal information may be added to that part of the Act to complete the information regime.

COSTS OF IMPLEMENTATION

The resource implications of any new proposal need to be kept in mind during its development and the need to balance the benefits of the legislation to the public against the costs of implementation has been recognised. We believe that our preferred method of implementation, through general legislation included in the OIA, is the least expensive. To review legislative powers to collect information, no doubt resulting in numerous amendments to ensure they were in line with the principles, would cost time and money for Departments, Parliamentary Counsel and Parliament itself, and finally would be no more effective than our proposals. The proposals primarily require a particular pattern of thinking by those who are collecting, using and holding personal information - a need to keep the privacy or confidentiality interests of the subject in mind at all stages of the processing of the information. What, then, are likely to be the costs?

a) There may be some extra interim printing costs (e.g. covering memos), to ensure that the requirements of Clause 23C are met. Not all present forms will meet the requirements, but this can be rectified at their next printing. Appendix X gives an example of the type of information that be incorporated into forms requesting information, particularly where the form is mailed to the subject for completion. Any costs here should be minimal, and non-recurring.

b) Redesigning of forms will be required in many cases - however as forms should always be carefully reviewed whenever they are reprinted, this cannot be said to a increased resource cost.

c) There will probably need to be some training or staff awareness programmes implemented, to ensure some understanding of the principles. But, as departments have ongoing staff development programmes for all staff these should be able to incorporate the requirements for collection and use of personal information. In fact, by making people aware of the issues they should be considering when collecting and using personal information it is likely better collection procedures will be used, only the necessary information acquired, and a better understanding developed between the agency and the subject of the information. There could be an improvement in the agency's public relations.

d) There may be some costs incurred in upgrading the security of electronic data systems in particular. This is not just the result of the implementation of the principles; the Interdepartmental Committee on Security has already published booklets on security of information in departments and organisations, which require certain standards to be met.

e) Costs incurred in any review investigation will be kept to a minimum, with the appeal procedure being with the Ombudsmens' Office rather than through the Court system.

f) The publication setting out personal information held, as required by Clause 23G, may cause some expense in the initial development. It will however, ensure that management throughout the whole agency becomes aware of all the systems that are in place, which could reduce the collection function. The publication can be as simple as the department wishes, providing it covers the requirements of clause 23G.

Chapter Three

PRIVACY AND OFFICIAL INFORMATION

What are the protections presently available in the Official Information Act which allow the withholding of official information of a personal nature, where it is considered that this is necessary?

INFORMATION ABOUT 'LEGAL' PERSONS

The Authority has already done a great deal of work on the protection available in the OIA for competitive commercial information, which is the bulk of information held about legal persons. This work led to the proposed amendments to ss.8 and 9 which are included in the Official Information Amendment Act 1987. These amendments also cover information that may not have a competitive commercial element, but which was supplied in confidence and if released, could effect future supply. The collection and use rules we are proposing be included in Part IV of the act will apply as much to legal persons as to natural persons.

INFORMATION ABOUT 'NATURAL' PERSONS

Interpretation of s.9(2)(a) of the Official Information Act is not easy. Just what does 'privacy of the natural person' mean in New Zealand? For instance, should Social Welfare reveal the address of a mother and children to the children's father, when he has been known to physically abuse the mother and there is a non-molestation order against him? How much information should be given about other job applicants to those appealing against an appointment? Should any other government agency than that which collected it, have access to personal information to use for the possible detection of criminal activity?

The Ombudsman has made two significant statements about the type of information that the term 'privacy of the natural person' will encompass. The information must not already be public knowledge, (cases 50 and 77, 5th Compendium of Ombudsmen Case Notes), and it must be of an intimate nature, (Report of the Chief Ombudsman on leaving office, October 1984 para 2.23 p.16).

Identification: Before it can be contended that a person's privacy is at stake it must be shown that the information which is sought will identify that person (Case No 7, 5th Compendium of Ombudsmen Case Notes). Even where there is the prospect of identification this may not be sufficient to obtain the protection of s.9(2)(a), judging from the following observation of the Ombudsman in Case No.7.

> "I noted, however, that I did not regard the mere identification of an individual as tantamount to an infringement of the privacy of that person although there could be some circumstances where disclosure of identity would amount to such an infringement."

Public knowledge: The question of the extent to which the information is public knowledge is difficult to answer. If the information can be obtained from a public register is it public although it has not been widely published? The law relating to trade secrets recognises that a secret may be no less a secret even if it has been given limited exposure. Ombudsman Case No 50 makes it clear that if a person has been named in an internal report in connection with a particular activity and is subsequently named publicly in connection with the same matter he or she will not be protected by section 9(2)(a). On the other hand where the person named in the report has not been publicly named the Ombudsman was prepared to find that his or her privacy should be protected under s.9(2)(a) without applying the test of whether the information was of an intimate nature.

Information of an "intimate nature": Once again it is difficult to draw the boundaries around this phrase. The ALRC Report No.11 (Canberra, 1979 "Unfair Publication: Defamation and Privacy"), gives some guidance in recommending that "sensitive facts" embrace -

> "... matter(s) relating or purporting to relate to the health, private behaviour, home life or personal or family relationships of the individual in circumstances in which the publication is likely to cause distress, annoyance or embarrassment to an individual... "

This suggests that a test for privacy under the Ombudsman's current approach of narrowing the ambit of the word to information of an intimate nature, would be whether the consequence of disclosure would be to "cause distress, annoyance or embarrassment to an individual ... " Case No. 70, 5th Compendium, lends some support to this test but confuses the issue by allowing privacy to extend to the expression of a person's views on an issue. In that case the telling factors were that the views were opinions of a personal nature on matters of morals and religion and that when provided there was no suggestion they would be published. The Ombudsman concluded that the people expressing personal views in submissions to the Minister of Education "would have been unlikely to respond to the Minister's invitation if they believed their views would be published."

Countervailing Public Interest: Where the first test has been met and there is an accepted case for non-disclosure on the basis that the information comes within the privacy ground, the next step is to weigh non-disclosure against the public interest in having the

information publicly available. While the starting point is the public interest, as expressed at section 4 of the OIA, it would seem that this is not exhaustive and a public interest reason may also be found outside section 4 grounds. This is evident from Case No 203, 6th Compendium, where the public interest was seen to correspond with the rights of the husband to have access to his children. In that case the husband had sought from Social Welfare Department the address of an estranged wife. It was decided by the department that in this instance the wife's privacy was outweighed by the greater public interest in the father's legal right of access to his children who resided with the mother.

Legislation: Privacy is a very difficult subject on which to legislate, because the matters that one person considers private in one situation, may not be considered so by another, or by the same person in a different situation. For instance, a person may not want friends and relatives to know about a sensitive medical condition, but be quite happy to discuss it with strangers in the medical profession, or with fellow sufferers.

While there are some overseas examples of what might be regarded as sensitive personal information, there is no general agreement on this. The OECD Guidelines "do not find it possible to define any set of data which are universally regarded as sensitive", although they state there should be an "affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data". European laws contain a variety of items that are considered sensitive, with no uniformity. The following list from the ALRC report on Privacy illustrates this:

- *race - Denmark, France, Norway;*
- *political affiliations or beliefs - Denmark, France, Luxembourg, Norway, Sweden;*
- *philosophical beliefs - France, Luxembourg;*
- *union affiliations - France, Luxembourg;*
- *religious beliefs - Denmark, Luxembourg, Norway, Sweden;*
- *skin colour - Denmark;*
- *sexual activities - Denmark, Norway;*
- *criminal records - Denmark, Luxembourg, Norway, Sweden;*
- *state of health - Denmark Norway;*
- *drink/drug abuse - Denmark, Norway, Sweden;*
- *credit-worthiness - Denmark;*
- *psychiatric problems - Sweden;*
- *receipt of social services - Sweden;*
- *'family intimacies' - Norway;*
- *medical records - Luxembourg.*

There is also the same diversity of approach in the Canadian federal legislation and that of the various provinces that have some form of privacy legislation. For instance, Ontario Bill 34, Clause 21, (See Appendix IX), has an extensive list of personal information the release of which would be presumed to constitute an unjustified

invasion of personal privacy. It also lists the matters to be taken into account by an agency when considering whether there is a public interest in release. The Quebec Act s.57, (see Appendix VII), instead states what is public information, so it might be assumed that anything not on that list, is private information. The Canadian Privacy Act, gives an extensive definition of 'personal information', and also specifies that information which it regards as in the public domain. (See Appendix VI.)

This divergence of approach to what is privacy, and how it should be protected, is no doubt because of cultural differences and, over time, our changed perceptions of sensitivity. It will also be influenced by what we perceive as our need for freedom of speech and of the press, and the value the community places on the free flow of information.

Despite the difficulties, the Authority believes that it could be helpful for requesters, suppliers and subjects of personal information to have a little clearer understanding of what is seen as the 'privacy of the natural person' and some consideration should be given to a possible expansion of s.9(2)(a). We have, therefore, drafted at this stage for discussion purposes only, a possible Clause 9A, which would replace the present s.9(2)(a). It attempts to state the public interest issues to be considered in deciding on the withholding of personal information, and to indicate to holders of the information, as well as users of the OIA, what should be considered when deciding on requests for such information. The collection and use rules in Part IV should also be taken into account. A clearer view of the reasons for withholding in Clause 9A, should also reduce the list of exceptions for use for other purposes required in Clause 23F. The expansion of s.9(2)(a) was not raised in our previous discussion document and we would ask those responding to us to give this matter careful consideration.

POSSIBLE NEW CLAUSE 9A WHICH WOULD EXPAND THE PRESENT SECTION 9(2)(a) AND STATE MATTERS THAT SHOULD BE TAKEN INTO ACCOUNT WHEN DETERMINING THE 'PUBLIC INTEREST' TEST IN RELATION TO THE PRIVACY OF THE NATURAL PERSON.

9A. REASONS FOR WITHHOLDING OFFICIAL INFORMATION RELATED TO NATURAL PERSONS - (1) Good reason for withholding official information exists, for the purpose of section 5 of this Act, if the making available of that information could reasonably be expected to constitute an invasion of the privacy of natural persons, including that of deceased natural persons, unless, in the circumstances of the particular case, the withholding of that information is outweighed by other considerations which render it desirable, in the public interest, to make that information available.

COMMENT

Sub-clause (1) repeats the present s.9(1) and includes with it s.9(2)(a).

(2) In determining whether, in a particular case, the withholding of the information is outweighed by the public interest, the Department or Minister of the Crown or organisation shall consider -

(a) the nature of the information that would be disclosed; and
(b) circumstances in which the information was obtained; and
(c) likelihood of the information being information that the person concerned would not wish to have disclosed without consent.

Particular consideration shall be given to -

(d) whether access is necessary to prevent or lessen a serious and imminent threat to the life or health or safety of the subject or any other person; or
(e) whether the information is relevant to a fair determination of rights affecting the person making the request; or
(f) whether the disclosure is desirable for the implementation of s.4(a) of this Act; or
(g) whether the disclosure is necessary for the maintenance of the law, including the prevention, investigation, and detection of offences.

COMMENT

Our first draft of this part of the clause was modelled on that of the Ontario Bill (Appendix IX) with a more specific list of public interest matters, together with a lengthy list of information, the disclosure of which (if not already publicly available), would be presumed to constitute an invasion of privacy of natural persons. It ended with a number of items that the clause was specifically not to apply to - in other words that information would be public information. This was primarily state sector salaries and certain contracts entered into by Government. To have such definitive lists, however, can lead to more problems than they solve, as argument takes place on whether the matters really are regarded in our society as 'invasions of privacy.' Neither do they readily take into account the different circumstances that we instanced in our discussion on the problem.

We finally took a general approach in sub-paragraphs (a) to (c), on matters that should be weighed when considering whether there was

a public interest in releasing information that might invade the privacy of a natural person. They are interests which the Australian Administrative Appeals Tribunal in Re John Chandra and the Department of Immigration and Ethnic Affairs, (an Access to Information case), said should be considered when deciding whether release of personal information would be 'unreasonable' in the circumstances.

The four more specific conditions of sub-paragraphs (d) to (g), cover particular public interests which we believe would be accepted by the community as reasons that might in certain cases outweigh the privacy of the individual. Sub-paragraphs (d) to (f) probably do not need explanation - they are self explanatory - but sub-paragraph (g) does. We would refer to our comments on proposed new section 23F, in Chapter Two of the booklet, where we discuss some of the issues regarding access to information for the 'maintenance of the law'. We mention the Canadian legislation that gives a discretion to the departmental head as to whether information is released in certain circumstances, and which we have used as a model. We trust that this will be given careful consideration by those responding to us on our proposals.

Chapter Four

COLLECTION AND USE LEGISLATION

Suggested New Sections to be Included in Part IV of the Official Information Act 1982

NOTE ON REFERENCES

In the comments on the clauses that follow -
- "IA" is the Information Authority's principles as published in "Personal Information and the Official Information Act - An Examination of the Issues". See Chapter Five.
- "OECD" is the Council of the OECD's "Guidelines Governing The Protection of Privacy and Transborder Data Flows of Personal Data", Part Two. See Appendix III.
- "ALRC" is the Australian Law Reform Commission's report on Privacy (Kirby Report), which listed privacy principles. See Appendix IV.
- "NSWPC" is the New South Wales Privacy Commission and the principles referred to are taken from their report "Privacy Issues and the Proposed National Identification Scheme - A Special Report", March 1986. See Appendix V.
- "Canadian Act" is the Privacy Act 1982. For sections referred to below, see Appendix VI.
- "Quebec Act" is the Access to Documents held by Public Bodies and the Protection of Personal Information Act 1984. For sections referred to below, see Appendix VII.
- "UK Act" is the Data Protection Act 1984. For Principles and a Guide to their Interpretation, incorporated in the Act, see Appendix II.
- "USA Act" is the Privacy Act 1974. For sections referred to below, see Appendix IIX.
- "Ontario Bill" is Bill 34, Freedom of Information and Protection of Individual Privacy, introduced on July 12 1985, and recently reported back for a 2nd Reading. For clauses referred to below, see Appendix IX.

COLLECTION AND USE OF PERSONAL INFORMATION

23A. **NEED FOR COLLECTION** - A Department or Minister of the Crown or organisation may collect personal information only if the need for it arises from the due exercise of the duties and responsibilities of that Department or Minister of the Crown or organisation.

COMMENT:

See IA/1, 2, 7, 8; Cf, OECD/7; ALRC/1; NSWPC/1; Canadian Act s.4; Quebec Act s.64; UK Act P/1, 2; USA Act/552a(e)(1); Ontario Bill Cl.35(2).

This is the fundamental question - is collection necessary to the activity of the agency? It brings into focus the competing interests of the State in the effective carrying out of the public interest, balanced against the privacy/confidentiality interest of the person concerned. This should be the starting point for consideration of whether the collection is justified or not. Any collection of personal information should have to clearly outweigh the privacy/confidentiality interests and the agency should be able to show the need for its collection. Collection is on a 'need to know' not a 'nice to know' basis. Information which is merely 'incidental to' or 'connected with' the purpose has no basis for collection.

We would refer to our discussions in Chapter Two on the Scope of the Legislation, and specifically our comments on self incrimination. The Public and Administrative Law Reform Committee also discussed this in their report on Statutory Powers of Entry. (They included as their Principle 12, the same Question Principle as in the Authority's suggested principles.) In commenting on the principle the Committee said "The privilege is expressly affirmed in comparatively few existing statutes. The Committee's view is that this should become the general rule and that where the privilege is negated, this should be clearly stated. A department should bear the onus of establishing that negation of the principle is clearly justified in the particular enactment." The Authority would support this.

A requirement that the information should be collected by lawful means has not been included - this goes without saying. No agency has the right to break the law.

23B. **MEANS OF COLLECTION** - (1) A Department or Minister of the Crown or organisation shall collect personal information directly from the person to whom it relates except -

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

COMMENT:

See IA/2, 3, 8. Cf. OECD/7; ALRC/1; NSWPC/1; Canadian Act s.5, UK Act P/1, 2; USA Act/552a(e)(2); Ontario Bill Cl.36.

Wherever possible in the interests of fairness and accuracy, information should be collected from the subject, particularly when the information may be used in decisions affecting that person. Only when the information is -

* *already publicly available; or*
* *the subject has authorised otherwise; or*
* *it would defeat the purpose of the collection; or*
* *it is to the benefit of the subject;*

should the collection be from third parties.

23C. **PERSON TO BE TOLD** - The person from whom the information is collected shall be told, except where it would prejudice the purpose of the collection -

(a) the purpose for which the information is being collected; and
(b) whether the collection of the information is required or is authorised by or under law, and whether disclosure by that person of such information is mandatory or voluntary; and
(c) the effects on that person, if any, of not providing all or any part of the requested information; and
(d) the categories of persons who will have access to the information; and
(e) the rights of access to and correction of personal information provided by this Act.

COMMENT:

See IA/1, 2, 3, 7, 8. Cf. OECD/9; ALRC/2; NSWPC/2; Canadian Act s.5; Quebec Act s.65; USA Act/552a(e)(3); Ontario Bill Cl.36(2).

The requirement to advise the above to the person the information is requested from, while primarily concerned with the Informing Principle (IA/3), will also contribute to -

> *IA/1 <u>necessity</u> for the information through having to clarify the purpose for which it is used;*
> *IA/2 <u>fair collection</u> as there is the need to justify the collection to the supplier and make known the powers to collect;*
> *IA/7 <u>objective reasons</u>, because having to clearly state why the information is needed and justify collection should make the ground for collection more objective;*
> *IA/8 <u>relevance</u> of purpose is also more likely to be achieved.*

An exception to the need to advise the person can only be given where it can be clearly shown that the purpose of the collection would be frustrated if the person providing the information was advised of the reasons for collection. While clause 23A still requires justification for the collection of this information, the matter of collection of what might be called 'intelligence records'

raises a number of issues. A chief characteristic of such records is that they are usually gathered for the purpose of taking adverse action against the subject of the information. The ones causing most difficulty within this context are the criminal and the security intelligence systems which probably have no controls other than those developed within the organisation itself, and only internal auditing systems. While one can assume that such systems will primarily be held by law enforcement agencies, this may not necessarily be so because the function of such systems does not lead to public announcement.

While we realise that requiring the application of the collection and use safeguards to such information would be to weaken its effectiveness, and therefore the functions of the agency collecting the information, we are also aware of the risk of abuse of the records, and the potential for considerable harm to the individual. We have at this stage provided for an exemption of the need to collect information from the subject or to advise the person from whom the information is collected where these would frustrate the purpose of the collection. We will be very interested in the response to these provisions.

23D. **HOLDERS AND USERS TO ENSURE INFORMATION SECURITY** - A Department or Minister of the Crown or organisation which holds or uses personal information shall take all reasonable steps to ensure the information is safeguarded against unauthorised access, alteration, use, disclosure or destruction.

COMMENT:

See IA/12. Cf. OECD/11; ALRC/4; NSWPC/4, Quebec s.69; UK Act P/8; USA Act/552a(e)(10).

There may be occasions when the holder of the information is not the user, hence the requirement that both are responsible for information security.

23E. **USERS TO ENSURE INFORMATION QUALITY** - A Department or Minister of the Crown or organisation which uses personal information shall take all reasonable steps to ensure, when the information is to be used, that it is accurate, up to date, complete and not misleading for the purpose for which it is to be used.

COMMENT:

See IA/5, 8, 10. Cf. OECD/8; ALRC/3, 7; NSWPC/3; Canadian Act s.6(2), Quebec Act s.72: UK Act P/4, 5; USA Act/552a(e)(5),(6); Ontario Bill Cl.37(2).

The onus to ensure information quality falls on the user, not the holder or collector, although this will often be the same person. If the information is being used by someone other than the holder and collector, it should be the users responsibility to check that the information is suitable for the purpose. When information has been collected for a purpose other than that for which it is being used, (see Clause 23F), it is quite likely not to be complete or up-to-date for that use. If there is a time gap between collection and use, even where the collector and user are the same person, there is need to check to ensure information quality. The ultimate responsibility for the quality of any personal information used, whether for the purpose collected or not, must be that of the user.

23F. **USE FOR OTHER PURPOSES** - (1) A Department or Minister of the Crown or organisation may use or allow the use of personal information, the use of which is not prohibited or regulated by any other enactment, for a purpose other than the purpose for which it was collected only if -

(a) the subject of the information has consented to the use; or

(b) the purpose is consistent with the purpose for which the information was obtained; or

(c) the information is available in accordance with Parts I and II of this Act; or

(d) the Department or Minister of the Crown or organisation believes on reasonable grounds that the use of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or some other person; or

(e) the use of the information for that other purpose is required or authorised by law; or

(f) the request, in writing, is made by an investigative body listed in the ..... Schedule of this Act, where the information is required for the maintenance of the law, including the prevention, investigation and detection of offences, and the request specifies the purpose and describes the information to be disclosed; or

(f) the information is to be used in aggregate form or for statistical or research purposes and will not be published in a manner that will identify any person.

(2) A record shall be kept by holders of personal information of any use made of that information for a purpose other than the purpose for which it was collected.

(3) Nothing in this section affects any power of a Court or other body acting judicially to require the production of evidence.

COMMENT:

See IA/8, 9, 11. Cf. OECD/10; ALRC/8; NSWPC/10,11: Canadian Act s.7, 8, 9, 67, 68, 69; Quebec Act s.53, 59, 60, 61, 61.1, 67, 68, 74; UK Act P/3; USA Act/552a(b),(c); Ontario Bill Cl.38, 39, 42.

This provision is probably the one most likely to raise difficult issues for holders, potential users, suppliers and subjects of information. While the purposes for which information is collected should be specified at the time of collection there may be justifiable reasons for use for other purposes which are in the interests of the subject, or where the public interest in that use outweighs privacy or confidentiality interests listed in the suggested clause 9A.

Wherever possible, other uses should only be allowed with the consent of the subject. There will be occasions, however, when there is no scope for that consent and where exceptions are justified. It is also important that the 'uses for other purposes' is in line with the reasons under the OIA for withholding personal information on third parties, whether they be natural or legal persons. Clause 23F therefore must be compatible with the suggested new clause 9A, as well as sections 9(2)(b) and (ba) enacted by the Official Information Amendment Act 1987. Clause 9A is concerned with reasons for refusing to release information on natural persons to third parties, whereas Clause 23F accepts that there can be occasions when there should be access to the information and states when and how these could occur.

The use of information for other purposes, and when the consent of the subject has not been obtained, is suggested as reasonable only when the information -

- *is needed for health or safety reasons (e.g. communicable diseases, certain industrial safety matters); or*
- *use will be consistent with the purpose of the original collection and may not have been known at the time of that collection (e.g. the use of animal ownership figures in an exotic disease outbreak to trace likely suspect properties); or*
- *is required by other laws (e.g. taxation), although these should be rare as all such purposes should have been advised at the time of collection. Collectors should know of any other laws that may require access to the information and take these laws into account when deciding on the justification for collection; these should therefore be advised to the person supplying the information; or*
- *is required for specific investigative purposes, primarily by the police.*

To ensure it is possible to trace uses of the information a record should be kept of those uses other than the ones for which the information was collected.

The prevention of computer matching, without sufficient justification, such as on fishing expeditions, is one of the main reasons for constraints on collection and use. When Parliament believes that such a matching programme is necessary, it should be provided for in primary legislation, which then allows the public to have a contribution to the debate through the Select Committee hearings on the Bill. Subclause (e) aims at preventing 'matching' unless it is specifically provided for by law.

Striking the right balance between the public and private interests in access to information for the 'maintenance of the law' is not easy. Should we allow any agency that may have a concern that there has been a possible infringement of the law, however minor, to have access to personal information to check that suspicion, or do we restrict it purely to investigatory bodies and set out rules by which they might request information? Do we make the release mandatory, or should it be at the discretion of the head of the agency concerned?

The Authority has taken the view that there should be a restriction on access to personal information, and that this type of 'fishing expedition' should not be permitted. Access for investigative purposes should be permitted only when there is reasonable cause to believe that the requested information is material to the investigation. We have used as a model for subclause (f), the Canadian Privacy Act that has a discretionary provision which does not grant federal investigative bodies any right of access to personal information. Rather, the provision leaves to the discretion of the head of the agency from which the information is requested the ultimate decision on disclosure, pursuant to a written request, which must specify the information being requested and the reason why it is wanted. Those investigatory bodies which may make requests are listed in a Schedule to the Privacy Act and information cannot be released in response to a vague and indeterminate inquiry. It would appear that to date there have been no major problems arising from the Canadian provision.

23G. **PUBLICATION SETTING OUT PERSONAL INFORMATION HELD** - A Department or Minister of the Crown or organisation holding personal information shall make available, in all its public offices, by the 31 March of each year an up to date publication that includes in respect of each Department or Minister of the Crown or organisation -

(1) the categories of files of personal information maintained; and

(2) the nature of the information contained in those files; and

(3) the purposes for which the information was obtained or compiled and is used; and

(4) the name or names of any other Department or Minister of the Crown or organisation or person to who the

information is disclosed and the purpose of such disclosure; and

(5) the steps that the person should take if he wishes to obtain access to personal information.

COMMENT:

See IA/15. Cf. OECD/12; NSWPC/5; Canadian Act s.11; Quebec Act s.76; USA Act/552a(e)(4); Ontario Bill Cl.41.

There is already a limited duty to provide some of this information in the Directory of Official Information (s.20 of the OIA) and this extends that duty in relation to personal files, whether on manual or electronic systems. It is not intended this more detailed publication be included in the Directory but that it be available at all public offices of an agency for perusal. Such a publication reinforces the collection and use requirements and should assist both the public and the agency with specification of requests.

23H. **APPLICATION PROVISION** - (1) Any provisions in any enactment in relation to the collection and use of personal information by a Department or Minister of the Crown or organisation shall be read subject to the provisions in ss.23A to 23G of this Act unless -

(a) the latter Act states it applies notwithstanding this Act; or

(b) the provision is specified in the ..... Schedule to this Act.

COMMENT:

Cf. Quebec s.168; USA Act/552a(q); Ontario Cl.60(2); New Zealand Local Government Official Information and Meetings Bill, Clause 53.

There are, as we have already indicated, a large number of statutes giving powers to collect and use personal information and these may raise a number of issues that will have to be considered by departments and organisations and brought to the attention of the Authority. The intention of this proposed legislation, however, is to ensure that where such statutes do not measure up to the Principles for collection and use and it is agreed that they should do so, the deficiencies are provided for in the OIA. To require the amendment of a large number of statutes to bring them into line with the Principles would be a time consuming and frustrating exercise.

There may also be some present legislation (e.g. to do with maintenance of the law) which Departments and organisations believe should be retained and stand outside the ambit of clauses 23A to 23G. If agencies believe they have a case for exempting their particular powers from the proposed legislation they should advise the Authority giving detailed reasons for such exemption. The

Authority will discuss these with the agency. Clause 23H ensures that clauses 23A to 23F prevail over any present or future provisions regarding collection or use unless the provision is specified in a Fourth Schedule to the OIA, or in future legislation it is specifically stated that "notwithstanding the Official Information Act" the provision would apply.

Chapter Five

THE PRINCIPLES AND THE PROPOSED LEGISLATION

The Authority's first discussion booklet concluded in Chapter 10 with a recommended set of general principles to govern the collection, use of and access to personal information. These principles follow with the comments showing how each is covered in the proposed legislation.

COLLECTION PRINCIPLES

The power of collection is considered to be fair and reasonable where it complies with the following principles:--

1. NECESSITY PRINCIPLE
   Personal information is not collected unnecessarily.

COMMENT:

Clause 23A requires the collection to be related directly to an activity of the collecting agency. Cl.23C requires the collector to state, except in special circumstances, the purpose for which the information is being collected. If that purpose does not seem to be necessary to the supplier then the Ombudsman may be asked to review the collection. Cl.23G requires each agency to publish details of categories of personal files and state the purpose the information was obtained. Being required to do all these should act as a restraint on unnecessary collection.

2. FAIR COLLECTION PRINCIPLE
   Personal information is obtained and processed fairly and lawfully.

COMMENT:

The process of obtaining and processing fairly and lawfully should require -

- the agency to be clear on what information is needed and why, (Cl.23A);

- that wherever possible the information be collected directly from the subject, (Cl.23B);

- that the subject and supplier of the information know why it is needed, (Cl.23C);

- that the supplier understand the powers of the agency to collect, and the effect of not providing the information, (Cl.23C).

3. INFORMING PRINCIPLE

The person that collects personal information takes reasonable steps to ensure that, before it is collected, or if that is not practicable, as soon as practicable after it is collected, the record-subject is told:-

(a) the purpose for which the information is being collected, unless that purpose is obvious;
(b) if the collection of the information is authorised or required by or under law - that the collection of the information is so authorised or required; and
(c) in general terms of the record-keepers usual practices with respect to disclosure of personal information of the kind collected.

COMMENT:

Clause 23B requires that the information be collected directly from the subject. Cl.23C requires the person the information is collected from (regardless of whether the subject or a third person), to be advised of the purpose of collection, the powers of the collection, the results of non-supply, who will have access, and the subjects rights of access.

4. PRECISE POWER PRINCIPLE

When exercising a statutory power of entry, the acts the official can perform, the question that s/he may ask once s/he has gained admission and the uses s/he may make of any information that s/he acquires following entry, is related to the purposes of the particular entry and is specified as precisely as possible.

COMMENT:

The proposed legislation does not contain controls on powers of entry as the Public and Administrative Law Reform Committee has already dealt with these in their 1983 report on Statutory Powers of Entry. Once an entry has been made, however, the new OIA provisions would apply.

5. RELEVANCE PRINCIPLE

A person should not collect personal information that is inaccurate or having regard to the purpose of collection is irrelevant, out of date, incomplete or excessively personal.

COMMENT:

Again Cl.23A constrains the indiscriminate collection of information, while the onus for accuracy, timeliness and completeness of information is that of the user. (Cl.23E). If the information is being used some time after collection, the timeliness and completeness may be out of the hands of the collector to

control. Therefore users have a responsibility to check the validity of information before using it.

6. THE QUESTION PRINCIPLE
The relationship between the privilege against self-incrimination and an officials power to ask questions should be clarified in respect of each separate power, preferably by expressly affirming the privilege.

COMMENT:

The principle is implicitly included in Cls.23A and 23C. We discuss in the commentary of Cl.23A the need for specific legislation if the principle is to be negated and we support the position taken by the Public and Administrative Law Reform Committee. Cl.23C which states that a person must be advised if collection of information is required by law, and of the penalty for not providing the information, also contributes to the principle.

7. THE OBJECTIVE BELIEF PRINCIPLE
The grounds for collection of personal information should be objective not subjective.

COMMENT:

This should be the result of Cl.23A which states that collection must arise "from the due exercise of the duties and responsibilities" of an agency; of Cl.23C(a) where the purpose of collection must be stated; and Cl.23G which requires publication of types of information collected and why. There are constraints in having to state clearly why information is needed, with the possibility of an appeal to the Ombudsman if the reason is apparently not justified.

USE (INCLUDING DISCLOSURE)

The Use of Personal Information is Proper Where it Complies with the following Principles-

8. RELEVANCE PRINCIPLE
It is used for a purpose to which it is relevant.

COMMENT:

The constraints on collection of information (Cls.23A, 23B, and 23C), combined with the requirements on quality (Cl.23E), and the constraints on use for other purposes (Cl.23F), all contribute to ensuring that the purpose the information is used for is relevant.

9. PURPOSE PRINCIPLE
It is used only for the purpose for which the information is

collected, or a purpose incidental to or connected with that purpose unless:-

(a) the record subject has consented to other use;

(b) the person using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person; or

(c) the use is required by or under law.

COMMENT:

Use for purposes other than that for which the information was obtained is restricted unless certain criteria are met. The exceptions here are covered in Cl.23F.

10. ACCURACY PRINCIPLE

The person who uses personal information takes reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

COMMENT:

Proposed Cl.23E requires the user to ensure information quality.

11. CONSENT PRINCIPLE

The record-keeper does not disclose the personal information about the subject to a third person unless:-

(a) the record-subject has consented to the disclosure

(b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or some other person; or

(c) the disclosure is required by or under law.

COMMENT:

These exceptions are covered in Cl.23F, Use for Other Purposes, and should be reinforced by Cl.9A (for natural persons), and Sections 9(2)(b) and (ba) of the OIA (for legal persons).

12. SECURITY PRINCIPLE

The record-keeper takes such steps as are in the circumstances reasonable, to ensure that personal information held by the record-keeper or under his control is securely stored and is not misused.

COMMENT:

Clause 23D requires holders and users of personal information to ensure it is safeguarded against security risks.

ACCESS PRINCIPLES

How persons may find out what Personal Information is held on them; and the steps necessary for information to be corrected.

13. RIGHT OF ACCESS
Where a person has in his possession or under his control records of personal information the record-subject should have access to those records.

COMMENT:

This is already provided for in Part IV, Right of Access to Personal Information, OIA.

14. POWER TO REQUEST CORRECTION
A person who has in his possession or under his control a record of personal information about another person should correct it so far as it is inaccurate, or having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, misleading, out-of-date, incomplete or irrelevant.

COMMENT:

The present s.26 of the OIA provides for this.

15. OPPORTUNITY TO KNOW OF INFORMATION HELD
The subject should be informed of the existence of personal information held, particularly where this information is of a disparaging nature and is to be used in decision making.

COMMENT:

The requirement in Cl.23G, that each agency annually publish the categories and nature of information held, the purposes for which it was obtained and who has access, will give a fairly good indication to a person of whether there is likely to be a file on that person. The requirements in Cls.23B and 23C would also assist. We have not included a mandatory requirement to advise each person that a file is held because of the administrative costs involved and that in most instances the subject will be aware of the file because the information was collected from that person.

16. INTERMEDIARY ACCESS
Where direct access is impracticable, or may be harmful to the subject, intermediary or third party access should be available.

COMMENT

Section 25 of the OIA provides for access to personal information by the authorised agent of the subject and this allows access in

circumstances where it may be impractical for the subject to view the material. In rare cases of potential harm to the subject from access to the information (usually a health risk), the agency normally provides the subject's doctor or lawyer with the information and he or she is able to advise their patient or client what it is believed is most appropriate. Section 27(d) of the OIA may be used to refuse information where harm to the subject is likely, but agencies prefer to assist the subject as much as they can and make use of intermediaries wherever this is appropriate.

Appendix I

EXAMPLES OF COMPULSORY POWERS OF COLLECTION OF PERSONAL INFORMATION IN NEW ZEALAND LEGISLATION

S.305A Customs Act 1966 as amended by s.13 of the 1976 (No.2) Amendment)	- empowers the Comptroller of Customs to prescribe forms e.g. a declaration by flight crew members which includes the health of persons on a flight.
S.74 Health Act 1956	- requires medical practitioners to supply to the Medical Officer of Health details of any notifiable infectious disease or suspected notifiable disease.
S.45 Medicines Act 1981	- permits any member of the Police to inspect or make copies of the records required to be kept by every person who manufactures, packs, sells or supplies medicines, in circumstances corresponding to retail sales.
S.17 Inland Revenue Department Act 1974	- a wide power is given to the Commissioner of Inland Revenue to require every person to furnish any information and produce for inspection any books, and documents which the Commissioner considers relevant for any purpose relating to the administration or enforcement of any of the Inland Revenue Acts.
S.17(1) Penal Institutions Act 1954	- empowers the photographing and fingerprinting of inmates.
S.187 Industrial Relations Act 1973	- requires every Union to supply to the Registrar of Industrial Unions an annual return which is to include certain specified information in respect of its officers, trustees and auditors.
S.25 Apprenticeship Act 1983	- when a contract of apprenticeship terminates for any reason, a statement of service of the apprentice is required to be sent by the employer to the District Commissioner of Apprenticeships.

S.5 Factories and Commercial Premises Act 1981	- empowers departmental inspectors to inspect, examine, take samples, photographs, tests; or copy or take notes of any records held, to ascertain whether the provisions of the Act have been or are being complied with.
S.60 Insolvency Act 1967	- places a duty on a bankrupt to give certain information to the Assignee including a complete and accurate list of his properties, creditors, and debtors.
S.43 Electoral Act 1956	- requires every person qualified to be registered as an elector, to make application in the prescribed form for registration as an elector.
S.33 Immigration Act 1964	- requires all persons entering and leaving NZ to complete a passenger arrival or departure card.
S.33 Beer Duty Act 1977	- empowers the Collector of Customs to question any person in respect of any document delivered to him in accordance with the Act.
S.52 Mental Health Act 1969	- requires the superintendent of a hospital to send to the Director of Mental Health, Health Department, certain personal information in respect of a committed patient.
S.82 Hospitals Act 1957	- the Director General of Health may at any time, by notice in writing, require any Hospital Board to furnish such information as may be specified; and s.62(f) of the Act enables the DG to obtain patient information for statistical purposes.
S.31 Statistics Act 1975	- places an obligation on the recipient of a request to provide information requested by the Government Statistician and this is the authority for obtaining a wide range of personal information.
Ss.12, 38 Commerce Act 1975	- empower the Commerce Commission to, amongst other things, require any person to produce books or documents

	in his possession or under his control.
S.7 Valuation of Land Act 1975	- requires the owner or occupier or manager of any land to answer any questions and generally supply all necessary information to enable a correct valuation to be made.
S.25 Higher Salaries Commissions Act 1977	- the Commissioner may require any person to furnish information concerning salaries and other conditions of employment.
S.73 Human Rights Commission Act 1977	- provides a power to compel information of any type in the course of an investigation by the Commission.
Reg.27 Kiwifruit Marketing Licensing Regulations 1977	- empowers the collection of details of plantings and production of each kiwifruit producer.
Ss.9,11 Maternal Mortality Research Act 1968	- requires the notification of maternal deaths by medical practitioners and pathologists and other information such as social and educational status, medical/ pathological categories.
Ss.34,35 Reserve Bank of New Zealand Act 1964	- provides the Bank with power to obtain information relating to the business of building societies, life insurance companies, finance companies, and mortgage market companies.
S.11(2)(f) Waterfront Industry Act 1976	- enables the Waterfront Industry Commission to collect details of cargos carried on ships worked by waterside labour and details of times of working.

Appendix II

UK DATA PROTECTION ACT 1984 THE PRINCIPLES AND INTERPRETATION

[The following principles and interpretation are included in the Act.]

THE PRINCIPLES

Personal data held by data users

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

2. Personal data shall be held only for one or more specified and lawful purposes.

3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

5. Personal data shall be accurate and, where necessary, kept up to date.

6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7. An individual shall be entitled -

   (a) at reasonable intervals and without undue delay or expense -
      (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
      (ii) to access to any such data held by a data user; and
   (b) where appropriate, to have such data corrected or erased.

Personal data held by data users or in respect of which services are provided by persons carrying on computer bureaux.

8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or

destruction of, personal data and against accidental loss or destruction of personal data.

INTERPRETATION OF THE PRINCIPLES

The First Principle

1. (1) Subject to sub-paragraph (2) below, in determining whether information was obtained fairly, regard shall be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed.

(2) Information shall in any event be treated as obtained fairly if it is obtained from a person who -

(a) is authorised by or under any enactment to supply it; or

(b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom;

and in determining whether information was obtained fairly there shall be disregarded any disclosure of the information which is authorised or required by or under any enactment or required by any such convention or other instrument as aforesaid.

The Second Principle

2. Personal data shall not be treated as held for a specified purpose unless that purpose is described in particulars registered under this Act in relation to the data.

The Third Principle

3. Personal data shall not be treated as used or disclosed in contravention of this principle unless -

(a) used otherwise than for a purpose of a description registered under this Act in relation to the data; or

(b) disclosed otherwise than to a person of a description so registered.

The Fifth Principle

4. Any question whether or not personal data are accurate shall be determined as for the purposes of section 22 of this Act but, in the case of such data as are mentioned in subsection (2) of that section, this principle shall not be regarded as having been contravened by reason of any inadequacy in the information there mentioned if the requirements specified in that subsection have been complied with.

[Note: s.22 deals with compensation for inaccuracy.]

The Seventh Principle

5. (i)Paragraph (a) of this principle shall not be construed as conferring any rights inconsistent with section 21 of this Act.

(ii) In determining whether access to personal data is sought at reasonable intervals regard shall be had to the nature of the data, the purpose for which the data are held and the frequency with which the data are altered.

(iii) The correction or erasure of personal data is appropriate only where necessary for ensuring compliance with the other data protection principles.

[Note: s.21 deals with right of access to personal data.]

Appendix III

OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART TWO - BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

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

Data Quality Principle

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

Purpose Specification Principle

9. The purposes for which personal data is collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:-

(a) with the consent of the data subject; or
(b) by the authority of law.

Security Safeguards Principle

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

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:-

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) to have communicated to him, data relating to him

(i) within a reasonable time;

(ii) at a charge, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is readily intelligible to him;

(c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measure which give effect to the principles stated above.

Appendix IV

AUSTRALIAN LAW REFORM COMMISSION - INFORMATION PRIVACY PRINCIPLES

[These Principles are listed in the ALRC (Kirby) Report on Privacy, Volume Two, Appendix A, pages 265/266.]

Collection of Personal Information

1. Personal information should not be collected by unfair or unlawful means, nor should it be collected unnecessarily.

2. A person who collects personal information should take reasonable steps to ensure that, before he collects it or, if that is not practicable, as soon as practicable after he collects it, the person to whom the information relates (the "record-subject") is told-

(a) the purpose for which the information is being collected (the "purpose of collection"), unless that purpose is obvious;

(b) if the collection of the information is authorised or required by or under law - that the collection of the information is so authorised or required; and

(c) in general terms, of his usual practices with respect to disclosure of personal information of the kind collected.

3. A person should not collect personal information that is inaccurate or, having regard to the purpose of collection, is irrelevant, out-of-date, incomplete or excessively personal.

Storage of Personal Information

4. A person should take such steps as are, in the circumstances, reasonable to ensure that personal information in his possession or under his control is securely stored and is not misused.

Access to Records of Personal Information

5. Where a person has in his possession or under his control records of personal information, the record-subject should be entitled to have access to those records.

Correction of Personal Information

6. A person who has in his possession or under his control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, misleading, out-of-date, incomplete or irrelevant.

Use of Personal Information

7. Personal information should not be used except for a purpose to which it is relevant.

8. Personal information should not be used for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose unless-

(a) the record-subject has consented to the use;

(b) the person using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of record-subject or of some other person; or

(c) the use is required by or under law.

9. A person who uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

Disclosure of Personal Information

10. A person should not disclose personal information to another person unless-

(a) the record-subject has consented to the disclosure;

(b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of record-subject or of some other person; or

(c) the disclosure is required by or under law.

Appendix V

PRIVACY COMMITTEE OF NEW SOUTH WALES - SUGGESTED INFORMATION PRIVACY PRINCIPLES

[These Principles are contained in the Privacy Committee's Special Report on "Privacy Issues and the National Identification Scheme", March 1986.]

1. Personal information to be contained in a record:

   (a) should not be collected by unlawful or unfair means;

   (b) should be collected only if the information is necessary for a lawful purpose which is specified in accordance with principles 2 and 5; and

   (c) should, wherever possible, when the information may be used in a decision making process that directly affects the subject individual, be collected directly from that individual.

2. Where - (a) a person (the collector) collects personal information for inclusion in a record; and

   (b) the information is solicited by the collector from the record subject the collector should, on the form which is used to collect the information or on a separate from that can be retained by the record subject, inform the record subject of -

   (i) the purpose for which the information is being collected;

   (ii) whether collection of the information is required or is expressly authorised by or under law, and whether disclosure by the record subject of such information is mandatory or voluntary;

   (iii) the effects on the record subject, if any, of not providing all or any part of the requested information; and

   (iv) the name of any person or agency to whom the information may be disclosed by the record keeper.

3. Where a person (the collector) collects personal information

to be included in a record, the collector should take all reasonable steps to ensure that, having regard to the purpose for which the information is collected:

(a) the information collected is relevant to that purpose and is accurate, up-to-date and complete; and

(b) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the record subject.

4. A record keeper who has possession or control of a record that contains personal information should take all reasonable steps to ensure that the record is safeguarded against such risks as unauthorised access, alteration, use, disclosure or destruction, and against accidental loss or destruction.

5. A record keeper who has possession or control of records that contain personal information should take reasonable steps to enable any person to ascertain:

(a) the categories of records maintained;

(b) the nature of the personal information contained in the records;

(c) the purposes for which the information was obtained or compiled;

(d) the categories of individuals to who personal information contained in the records relates;

(e) the categories of sources of personal information contained in the records;

(f) the purposes for which information contained in the records is used;

(g) the name of any person or agency to whom the information contained in the records is disclosed and the purpose of such disclosure;

(h) The steps that the person should take if he/she wishes to obtain access to a record of personal information that relates to him/her;

(i) the policies and practices of the record keeper regarding storage, retrievability, access controls, retention and disposal of the record; and

(j) the title and business address of the record keeper.

6. Where a record keeper has possession or control of a record that contains personal information, the record subject should be entitled to have access to that record.

7. A record keeper who has possession or control of a record that contains personal information should:

(a) take all reasonable steps to ensure, by making appropriate corrections, deletions and additions, that the record:

(i) is accurate, up-to-date, complete and not misleading; and

(ii) is relevant to the purpose for which the information was collected, or for which the information may be used in accordance with principle 10: and

(b) permit the record subject to attach to the record his concise statement reflecting any corrections, deletions or additions requested but not made.

8. A record keeper who has possession or control of a record that contains personal information should not use that information without taking all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, complete and up-to-date.

9. A record keeper who has possession or control of a record that contains personal information should not use the information for a purpose other than the purpose for which the information was collected unless:

(a) the record subject has consented in writing to use of the information for that other purpose;

(b) the record keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the record subject or of some other person; or

(c) use of the information for that other purpose is required or is expressly authorised by or under law.

10. A record keeper who has possession or control of a record that contains personal information should not disclose the information to a person other than the record subject unless:

(a) the record subject has consented in writing to the disclosure;

(b) the record keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the record subject or of some other person; or

(c) the disclosure is required or is expressly authorised by or under law.

Appendix VI

CANADA — PRIVACY ACT 1982

[The following sections from the Privacy Act have been referred to for comparative purposes in the discussions on the proposed collection and use legislation, and the aspects of privacy of the natural person.]

3. INTERPRETATION

'personal information' means information about an identifiable individual that is recorded in any form including, without restricting the generality of the forgoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.

[The Act then goes on to list information that is not 'personal', primarily covering the salary, designation and responsibilities of public officials, details of particular contracts with individuals, discretionary benefits and licences or permits, and information on people dead for more that 20 years.]

COLLECTION, RETENTION AND DISPOSAL OF PERSONAL INFORMATION

Collection of personal information

4. No personal information shall be collected by a government institution unless it relates directly to an operating programme or activity of the institution.

Personal information to be collected directly

5. (1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorises otherwise or where personal information may be disclosed to the institution under subsection 8(2).

Individual to be informed of purpose

(2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.

Exception

(3) Subsections (1) and (2) do not apply where compliance therewith might

(a) result in the collection of inaccurate information; or

(b) defeat the purpose or prejudice the use for which information is collected.

Accuracy of personal information

6. (2) A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.

PROTECTION OF PERSONAL INFORMATION

Use of personal information

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution

except

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).

Disclosure of personal information

8. (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where personal information may be disclosed

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorises its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

(f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the government of a foreign state, an international organisation of states or an international organisation established by the governments of states, or any institution of any such government or

organisation, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;

(h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;

(i) to the Public Archives for archival purposes;

(j) to any person or body for research or statistical purposes if the head of the government institution

(i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

(k) to any association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;

(l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

Personal information disclosed by Public Archives

(3) Subject to any other Act of Parliament, personal information under the control of the Public Archives that has been transferred to the Public Archives by a government institution for archival or historical purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes.

Copies of requests under paragraph (2)(e) to be retained

(4) The head of a government institution shall retain a copy of every request received by the government institution under paragraph (2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make such copies and records available to the Privacy Commissioner.

Notice of disclosure under paragraph (2)(m)

(5) The head of a government institution shall notify the Privacy Commissioner in writing of any disclosure of personal information under paragraph (2)(m) prior to the disclosure where reasonably practicable or in any other case forthwith on the disclosure, and the Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to whom the information relates of the disclosure.

Record of disclosure to be retained

9. (1) The head of a government institution shall retain a record of any use by the institution of personal information contained in a personal information bank or any use or purpose for which such information is disclosed by the institution where the use or purpose is not included in the statements of uses and purposes set forth pursuant to subparagraph 11(1)(a)(iv) and subsection 11(2) in the index referred in section 11, and shall attach the record to the personal information.

Record forms part of personal information

(2) For the purposes of this Act, a record retained under subsection (1) shall be deemed to form part of the personal use to which it is attached.

Consistent uses

(3) Where personal information in a personal information bank under the control of a government institution is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by the institution but the use is not included in the statement of consistent uses set forth

pursuant to subparagraph 11(1)(a)(iv) in the index referred to in section 11, the head of the government institution shall

(a) forthwith notify the Privacy Commissioner of the use for which the information was used or disclosed; and

(b) ensure that the use is included in the next statement of consistent uses set forth in the index.

PERSONAL INFORMATION INDEX

Index of personal information

11. (1) The designated Minister shall cause to be published on a periodic basis not less frequently than once a year, an index of

(a) all personal information banks setting forth, in respect of each bank,

(i) the identification and a description of the bank, the registration number assigned to it by the designated Minister pursuant to paragraph 71(1)(b) and a description of the class of individuals to whom personal information contained in the bank relates,

(ii) the name of the government institution that has control of the bank,

(iii) the title and address of the appropriate officer to whom requests relating to personal information contained in the bank should be sent,

(iv) a statement of the purposes for which personal information in the bank was obtained or compiled and a statement of the uses consistent with such purposes for which the information is used or disclosed,

(v) a statement of the retention and disposal standards applied to personal information in the bank, and

(vi) an indication, where applicable, that the bank was designated as an exempt bank by an order under section 18 and the provision of section 21 or 22 on the basis of which the order was made; and

(b) all classes of personal information under the control of a government institution that are not contained in personal information banks, setting forth in respect of each class

(i) a description of the class in sufficient detail to facilitate the right of access under this Act, and

(ii) the title and address of the appropriate officer for each government institution to whom requests relating to personal information within the class

should be sent.

Statement of uses and purposes

(2) The designated Minister may set forth in the index referred to in subsection (1) a statement of any of the uses and purposes, not included in the statements made pursuant to subparagraph (1)(a)(iv), for which personal information contained in any of the personal information banks referred to in the index is used or disclosed on a regular basis.

Index to be made available

(3) The designated Minister shall cause the index referred to in subsection (1) to be made available throughout Canada in conformity with the principle that every person is entitled to reasonable access to the index.

OFFENCES

Obstruction

67. (1) No person shall obstruct the Information Commissioner or any person acting on behalf or under the direction of the Commissioner in the performance of the Commissioner's duties and functions under this Act.

Offence and punishment

(2) Every person who contravenes this section is guilty of an offence and liable on summary conviction to a fine not exceeding one thousand dollars.

GENERAL

Act does not apply to certain materials

68. This Act does not apply to

(a) published material or material available for purchase by the public;

(b) library or museum material made or acquired and preserved solely for public reference or exhibition purposes; or

(c) material placed in the Public Archives, the National Library or the National Museums of Canada by or on behalf of persons or organisations other than government institutions.

Confidence of the Queen's Privy Council

69. (1) This Act does not apply to confidences of the Queen's Privy Council for Canada, including, without restricting the generality of the forgoing

(a) memoranda the purpose of which is to present proposals or recommendations to Council;

(b) discussion papers the purpose of which is to present

background explanations, analyses of problems or policy options to Council for consideration by Council in making decisions;

(c) agenda of Council or records recording deliberations or decisions of Council;

(d) records used for or reflecting communications or discussions between Ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy;

(e) records the purpose of which is to brief Ministers of the Crown in relation to matters that are before, or are proposed to be brought before, Council or that are the subject of communications or discussions referred to in paragraph (d);

(f) draft legislation; and

(g) records that contain information about the contents of any record within a class of records referred to in paragraphs (a) to (f).

Definition of "Council"

(2) For the purposes of subsection (1), "Council" means the Queen's Privy Council for Canada, committees of the Queen's Privy Council for Canada, Cabinet and committees of Cabinet.

Exception

(3) Subsection (1) does not apply to

(a) confidences of the Queen's Privy Council for Canada that have been in existence for more than twenty years; or

(b) discussion papers described in paragraph (1)(b)

(i) if the decisions to which the discussion papers related have been made public; or

(ii) where the decisions have not been made public, if four years have passed since the decisions were made.

Appendix VII

QUEBEC – ACCESS TO DOCUMENTS HELD BY PUBLIC BODIES AND THE PROTECTION OF PERSONAL INFORMATION ACT 1984

[The following sections from the Act have been referred to for comparative purposes in the discussions in Chapter II and Chapter IV]

CONFIDENTIALITY OF NOMINATIVE INFORMATION

Confidential

53. Nominative information is confidential unless the person the information concerns authorises its disclosure.

Minor

In the case of a minor, the person having parental authority also may authorise the disclosure.

Public Information

57. The following is public information:

(1) the name, title, duties, classification, salary, address and telephone number at work of a member of a public body or of the board of directors of a public body;

(2) the name, title, duties, address and telephone number at work of a member of the personnel of a public body;

(3) information concerning a person as a party to a service contract entered into with a public body, and the terms and conditions of the contract;

(4) the name of a person deriving an economic benefit granted by a public body by virtue of a discretionary power, and any information on the nature of that benefit.

However, the information contemplated in the first paragraph is not public information where its disclosure would be likely to hinder or impede the work of a person responsible under the law for the prevention, detection or repression of crime.

Signature

59. In no case may nominative information be released by a public body, without the consent of the person concerned, except in the following cases and strictly on the following conditions:

(1) to the attorney of that body if the information is required for the purposes of a prosecution for an offence against an Act administered by that body or to

the Attorney General, if the information is required for the purposes of a prosecution for an offence against an Act applicable in Quebec;

(2) to the attorney of that body, or to the Attorney General where he is acting as the attorney of that body, if the information is required for purposes of judicial proceedings other than those contemplated in paragraph 1;

(3) to a person responsible by law for the prevention, detection or repression of crime or statutory offences, if the information is required for the purposes of a prosecution for an offence against an Act applicable in Quebec;

(4) to a person to whom the information must be disclosed because of the urgency of a situation that threatens the life, health or safety of the person concerned;

(5) to a person authorised by the Commission d'acces a l'information, in accordance with section 125, to use the information for study, research or statistics purposes;

(6) to the Keeper of the Archives nationales du Quebec, in accordance with the Archives Act;

(7) to the Bureau de la statistique du Quebec, according to law;

(8) to a body or agency, in accordance with sections 61, 61.1, 67 and 68.

Prior ascertainment

60. Before agreeing to the release of nominative information pursuant to paragraphs 1 to 3 of section 59, a public body must ascertain that the information is required for the purposes of a prosecution or proceedings contemplated in the said paragraphs.

Prior ascertainment

In the case contemplated in paragraph 4 of the said section, the body must, similarly, ascertain that an urgent and dangerous situation exists.

Refusal

Where a public body has not ascertained that the information is required for such purposes or, where such is the case, that an urgent and dangerous situation exists, the public body must refuse to release the information.

Record of request

Where a public body agrees to release nominative information following a request made pursuant to paragraphs 1 to 4 of section 59, the person in charge of the protection of the personal information within the public body must record the request.

Police force

61. A police force may, without the consent of the person

concerned, release nominative information to another police force.

61.1 A public body may, without the consent of the person concerned, release nominative information to another public body to allow it to impute to the account of the person concerned an amount that the law requires to be withheld or paid.

In the case of this section, the public body to which the nominative information may be released shall inform the Commission of the kinds of information that will be furnished to it.

COLLECTION, KEEPING AND USE OF NOMINATIVE INFORMATION

Unnecessary information

64. No person may, on behalf of a public body, collect nominative information if it is not necessary for the carrying out of the attributions of the body or the implementation of a programme under its management.

Prior identification and information

65. Every person who, on behalf of a public body, collects nominative information from the person concerned or from a third person must first identify himself and inform him

(1) of the name and address of the public body on whose behalf the information is being collected;

(2) of the use to which the information will be put;

(3) of the categories of persons who will have access to the information;

(4) of the fact that a reply is obligatory, or that it is optional;

(5) of the consequences for the person concerned or, as the case may be, for the third person, in case of a refusal to reply;

(6) of the rights of access and correction provided by law.

Regulation

The rules according to which nominative information is to be collected are prescribed by government regulation.

Exception

This section does not apply to judicial inquiries or to any investigation or report made by a person responsible by law for the prevention, detection or repression of crime or statutory offences.

Written agreement

67. Where the law, otherwise than in the cases contemplated in sections 59, 61 and 61.1 of this Act,

authorises a public body to release nominative information to another public body without the consent of the person concerned, the release must be made under the terms of a written agreement between the bodies.

Opinion of Commission

Where nominative information, the release of which is thus authorised, is required for the carrying out of an Act, a public body may, if there is no agreement, apply to the Commission for its opinion on the content of the proposed agreement.

Opinion of Commission

After giving the other public body an opportunity to submit its observations, the Commission shall give its own opinion to the bodies concerned.

Binding order

If, after considering the opinion, the proposed agreement is not accepted, the Commission may, at the request of one of the bodies concerned, determine the content of the agreement and submit it to the Government for approval. The order binds the public bodies concerned and constitutes an agreement for the purposes of this Act.

Disclosure agreement

68. A public body may make an agreement with another public body or in accordance with the law, with a government other than that of Quebec, an international organisation or an agency of such a government or organisation, to allow the disclosure of nominative information for the carrying out of an Act or for an investigation.

Disclosure agreement

A public body may also make an agreement with a person or a private body to allow the release of a list of names of natural persons or information allowing them to be identified.

[not in force]

Confidentiality

69. Every agreement under section 67 or 68 must provide for the necessary measures to ensure the confidentiality of the nominative information contemplated in the agreement.

Accuracy

72. Every public body must see to it that the nominative information kept by it is up to date, accurate and complete so as to serve the purposes for which it is collected.

Record

74. Every examination of a personal information file must be recorded.

Content

The record must indicate the name of the person concerned in the information being sought, the name and

function of the person examining the file, and, as the case may be, of the person having made the request, and the purpose for which it is examined. The public body must keep the record for at least two years.

Declaration

76. The establishment of a file must be the subject of a declaration to the Commission.

Content

The declaration must contain the following indications:

(1) the title of the file, the kind of information it contains, the use to which the information is to be put, the method by which the file is maintained and, where such is the case, the identification of the computer programmes used;

(2) the source of the information entered in the file;

(3) the categories of persons concerned in the information entered in the file;

(4) the categories of persons who have access to the file in carrying on their duties;

(5) the security measures taken within the public body to ensure the confidentiality of the nominative information and its use according to the purposes for which it was collected;

(6) the title, address and telephone number of the person in charge of protection of personal information;

(7) the modalities of access to the file of the person concerned;

(8) any other indication prescribed by government regulation.

Rules

The declaration must be made in accordance with the rules established by the Commission.

GENERAL PROVISIONS

Precedence

168. The provisions of this Act prevail over any contrary provision of a subsequent general law or special Act unless the latter Act expressly states that it applies notwithstanding this Act.

Appendix IIX

UNITED STATES OF AMERICA — PRIVACY ACT 1974

[The following sections from the Act have been referred to for comparative purposes in the discussions in Chapter II and Chapter IV.]

S.552A (b) CONDITIONS OF DISCLOSURE - No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be -

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties:

(2) required under section 552 of this title:

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (c)(4)(J) of this section:

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13:

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable:

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government or for evaluation by the Archivist to determine whether the record has such value:

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the records specifying the particular portion desired and the law enforcement activity for which the record is sought:

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last know address of such individual:

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee:

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;

(11) pursuant to the order of a court of competent jurisdiction, or

(12) to a consumer reporting agency in accordance with section 3711(f) of title 31.

S.552a (c) ACCOUNTING OF CERTAIN DISCLOSURES - Each agency, with respect to each system of records under its control, shall -

(1) except for disclosures made under subsection (b)(1) or (b)(2) of this section, keep an accurate accounting of -

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section: and

(B) the name and address of the person or agency to whom the disclosure is made:

(2) retain the accounting made under paragraph (1) of subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made:

(3) except for disclosures made under (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request: and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

S.552a "(e) AGENCY REQUIREMENTS - Each agency that maintains a system of records shall -

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President:

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual -

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary:

(B) the principal purpose or purposes for which the information is intended to be used:

(C) the routine uses which may be made of the information as published pursuant to paragraph (4)(I) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include -

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use:

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

S.552a (e) (10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; and

S.552a (q) (1) EFFECT OF OTHER LAWS - No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section."

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

Appendix IX

ONTARIO — FREEDOM OF INFORMATION AND PROTECTION OF INDIVIDUAL PRIVACY BILL 1986

[The following Clauses from the Bill have been referred to for comparative purposes in the discussions in Chapter II and Chapter IV.]

COLLECTION AND RETENTION OF PERSONAL INFORMATION

Collection of personal information

35. (2) No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

Manner of collection

36. (1) Personal information shall only be collected by an institution directly from the individual to whom the information relates unless

(a) the individual authorizes another manner of collection;

(b) the personal information may be disclosed to the institution concerned under section 39;

(c) the Commissioner has authorized the manner of collection under clause 55(c);

(d) the information is in a report from a reporting agency in accordance with the Consumer Reporting Act; R.S.O.1980

(e) the information is collected for the purpose of the conduct of a proceeding or a possible proceeding before a court or judicial or quasi-judicial tribunal;

(f) the information is collected for the purpose of law enforcement; or

(g) another manner of collection is authorized by or under a statute.

Notice to individual

(2) Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

Standard of accuracy

37. (2) The head of a public institution shall ensure that personal information on the records of the institution is not used unless it is reasonably accurate and up to date.

USE AND DISCLOSURE OF PERSONAL INFORMATION

Use of personal information

38. An institution shall not use personal information in its custody or under its control except

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) for the purpose for which it was obtained or compiled or for a consistent purpose; or

(c) for a purpose for which the information may be disclosed to the institution under section 39.

Where disclosure permitted

39. (1) An institution shall not disclose personal information in its custody or under its control except -

(a) in accordance with Part II;

(aa) where the person to whom the information relates has identified that information in particular and consented to its disclosure;

(ab) for the purpose for which it was obtained or compiled or for a consistent purpose;

(b) where disclosure is made to an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions;

(c) for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty agreement or arrangement thereunder;

(d) where disclosure is by a law enforcement institution,

(i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority; or

(ii) to another law enforcement agency in Canada.

(e) where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

(f) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

(g) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is

injured, ill or deceased;
(h) to a member of the Legislative Assembly who has been authorized by a constituent to whom the information relates to make an inquiry on the constituent's behalf or, where the constituent is incapacitated, has been authorized by the next of kin or legal representative of the constituent;
(i) to the Provincial Auditor;
(j) to the Ombudsman;
(k) to the responsible minister;
(l) to the Information and Privacy Commissioner;
(m) to the Government of Canada in order to facilitate the auditing of shared cost programmes;
(n) to the Archives of Ontario; and
(o) to Statistics Canada.

PERSONAL INFORMATION BANKS

Personal information bank index

41. (1) The responsible minister shall publish at least once each year an index of all personal information banks setting forth, in respect of each personal information bank
(a) its name and location;
(b) the legal authority for its establishment;
(c) the types of personal information maintained in it;
(d) the principal uses of the personal information and the typical categories of users to whom disclosures from the system are made;
(e) any other uses and purposes for which personal information in the personal information bank is used or disclosed on a regular basis;
(f) the categories of individuals for whom records are maintained in the system;
(g) the policies and practices applicable to the system with respect to storage, retrievability, access controls, retention and disposal of personal information maintained in the system; and
(h) the title, business address and business telephone number of the official responsible for the operation of the personal information bank.

Retention of record of use

42. (1) A head shall retain a record of any use by the institution of personal information contained in a personal information bank and of any use or purpose for which the information is disclosed where the use and purpose is not included in the statements of uses and purposes set forth under clauses 41(1)(d) and (e) and shall attach or link the record of use to the personal information.

Record of use forms part of attached or linked information

(2) A record retained under subsection (1) part of the personal information to which it is personal

Notice and publication

(3) Where the personal information in a personal information bank under the control of an institution is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by the institution but the use is not one of the uses included under clauses 41(1)(d) and (e) the head shall

(a) forthwith notify the responsible minister of the use or disclosure; and

(b) ensure that the use is included in the index.

Other Acts

60. (2) This Act prevails over a confidentiality provision in any other Act unless the other Act specifically provides otherwise.

Appendix X

EXAMPLES OF WORDING ON FORMS

The following are examples of the type of notification that should be given, in addition to other explanatory material, on forms or in covering letters that request the supply of personal information. Departments should state clearly the specific powers and reasons for collection, and who will have access to the information.

Example 1

ANIMAL STATISTICS

Notes:

1. The _____ Act, section ___, authorises the Department to collect annual statistics on population numbers and disease incidence of _____ for the purpose of national economic planning. Supply is mandatory and you can be fined up to $100.00 if the information requested is not advised to the Department by _____.

2. Aggregated statistics which do not identify individual owners are made public to assist bodies such as the Producer Boards, Freezing Companies and Government agencies in their economic and financial planning. Unless good reason is established under s.23F of the Official Information Act, individual questionnaires will only be seen by Departmental staff directly concerned with the analysis.

3. Under the Official Information Act, Part IV, you may ask to see any personal information the Department is holding about you.

Example 2

APPLICATION FOR REGISTRATION OF A _____

Notes:

1. Registration is required under s._____ of the _____Act, to provide for the control and monitoring of the _____ Industry as set out in the Act. There is a maximum fine of $2500.00 for operating a _____ without registration.

2. Names and address of all those registered, as required by s._____of the Act, will be publicly available at the Registrar's office during normal business hours. Unless good reason is established under s.23F of the Official Information Act 1982, access to further information will be restricted to those Departmental staff concerned with the registration and monitoring process.

3. Under Part IV of the Official Information Act you may ask to see any personal information the Department is holding about you. Should you wish to do so write to the above address.