A PRIVACY ACT FOR NEW BRUNSWICK

A DISCUSSION PAPER

Department of Justice

July 1996

TABLE OF CONTENTS

INTRODUCTION

Since 1987 the government of New Brunswick has been a strong promoter of the emerging information technologies, and has mandated its departments and agencies to use these technologies to provide better and more efficient services. However, it is widely recognized both inside and outside government that the use of these technologies raises privacy concerns. The government has undertaken several studies of these issues in the last few years, notably that of the New Brunswick Government Task Force on Data Sharing and Protection of Personal Privacy.

The Task Force reported in 1994. Its Report, *Protecting Privacy in an Information-Sharing Environment*, recommended that the government adopt as policy a *Personal Privacy Code* to provide a consistent and comprehensive guide to its information management practices. In accepting this recommendation, the government left open the option that it might later decide to adopt legislation, rather than a policy, as the means of protecting personal privacy.

In the 1995 provincial election, privacy legislation was among the subjects addressed in the election platform of the provincial Liberal Party:

> . . . in a new mandate, a Liberal Government would . . . prepare a new Privacy Act to ensure the protection and confidentiality of personal information in the possession of the government of New Brunswick. In drafting the bill, public hearings will be held to secure the views of New Brunswickers. (*Moving Ahead Together*, para.79.)

In the Throne Speech for the 1996 legislative session the government announced that it would table a discussion paper in the Legislative Assembly as part of this process. By unanimous agreement of the Legislative Assembly on April 19th 1996, the discussion paper, when tabled, is to stand referred to the Law Amendments Committee, which is to examine and inquire into the matter of privacy legislation, to conduct public hearings into the matter, and to report back to the Legislative Assembly. This paper has been prepared by the Department of Justice for the purpose of the proceedings in the Legislative Assembly. It contains proposals for the content of a Privacy Act which will protect the confidentiality of personal information in the possession of the provincial government and its agencies.

The protection of privacy in the information age became a matter of concern as early as the 1970s. In 1981, the Organization for Economic Cooperation and Development (OECD) issued Guidelines for the protection of personal privacy in the information context. These are now considered the basic principles of "fair information practices". There are eight Guidelines, which can be summarized as follows:

- the collection limitation principle: information should be collected by lawful and fair means with the knowledge and consent of the data subject;

- the data quality principle: personal information should be kept accurate and up to date;

- the purpose specification principle: the purpose for which data is collected should be specified to the data subject at the time of collection, and subsequent uses of the data should be limited to that purpose or to a consistent purpose;

- the use limitation principle: personal data should not be used or disclosed for purposes other than those specified in the previous paragraph, except with the consent of the data subject or by the authority of law;

- the security safeguards principle: personal information should be protected against unauthorized access by reasonable safeguards;

- the openness principle: means should be readily available for people to discover what data about them is being kept, and for what purpose;

- the individual participation principle: people should have the right to see the information about them and to request corrections, if necessary; and

- the accountability principle: a data-holding institution should appoint a data controller to be accountable for complying with measures that give effect to these principles.

The aim of the OECD Guidelines was international harmonization of data protection laws in order to facilitate trade in information between member nations. Canada subscribed to the Guidelines in 1984, and the Guidelines form the basis of the privacy legislation that now exists at the federal level and in six of the provinces, as well as of New Brunswick's *Personal Privacy Code*.

The Guidelines contain "Principles of National Application", summarized above, which are intended to be applied within member countries of the OECD, and "Principles of International Application", which govern the relations between signatory states. Central to the "Principles of International Application" is the rule that the transborder flow of personal information will be restricted or refused to countries that do not either legislate the national principles or provide for an "equivalent" level of privacy protection.

In a law passed in 1995 by the European Parliament, the European Union has elaborated further on the need for the protection of personal privacy in the processing of personal information, and on the need for harmonization of privacy protection laws between member states. This law, the EU "Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", fine tunes the privacy protection principles first enunciated in the OECD Guidelines, and reaffirms in its Preamble both the importance of privacy protection to the free exchange of information and the idea that " . . . the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited."

The Privacy Act proposed by this discussion paper is based on the OECD Guidelines as they have been interpreted and elaborated in the subsequent legislation of other Canadian provinces, in the EU law and in the *Personal Privacy Code*. At the same time, this discussion paper acknowledges, as did the report of the Task Force on Data Sharing and Protection of Personal Privacy, the need for governments to take advantage of technologies to eliminate waste and duplication within government, to streamline bureaucratic procedures, to prevent fraud or misuse of programs, and to provide better services. The proposed Privacy Act tries to balance the competing interests at play in the controversial area of privacy protection.

The proposed Act also takes into account developments in Canadian constitutional law and common law relating to privacy. On the constitutional front, section 8 of the Canadian Charter of Rights and Freedoms protects citizens against "unreasonable search and seizure". The Supreme Court of Canada has stated that this includes the right to be free of unreasonable search and seizure of one's personal information (*R. v. Dyment*, [1988] 2 S.C.R. 417). Exactly what will amount to a "search" or "seizure" of personal information remains to be examined further by the courts; the case-law to date indicates that those words are not restricted to their most obvious meanings in the context of criminal investigations, and legal debate is likely to continue for some time about how far they may apply to other forms of information-gathering or information-handling that governments engage in. What does emerge from the cases at present, however, is that the objective of section 8 is that governments must respect the citizen's "reasonable expectation of privacy". By observing, therefore, "reasonable expectations of privacy", governments can avoid the danger of doing anything that would be considered to be an "unreasonable" search or seizure in the context of section 8.

As for common law developments, in *McInerney v. McDonald* (1992), 126 N.B.R. (2d) 271, the Supreme Court of Canada held that a patient's own medical information could not be withheld from the patient unless serious harm would come to him or her through being given access to the information. The Court held that, no matter what the source of the personal information, a doctor holds personal medical information in trust for the patient. Quoting from *R. v. Dyment*, above, the Court noted that information about one's body "remains in a fundamental sense one's own, for the individual to communicate or retain as he or she sees fit." Quoting further from the federal *Report of the Task Force on Privacy and Computers* (1972), the Court agreed that the individual maintains a "basic and continuing interest in what happens to this information, and in controlling access to it".

We live in an information age, and our personal information is subject to many competing pressures, from our constitutional right to privacy and our right to access our own personal information, to the legitimate need of government to manage information in the most efficient way for the overall betterment of society. This discussion paper proposes a Privacy Act which aims to achieve a fair balance between all these interests.

A PROPOSED PRIVACY ACT FOR NEW BRUNSWICK

1 Interpretation and Application

A Privacy Act provides a legislated code of conduct, in the form of general principles and exceptions, to guide the personal information management practices of those to whom it applies. Two preliminary matters arise that together define the scope of a Privacy Act. These are: To whom will the Act apply? and, What is meant by "personal information"? These questions are answered in section 1 of this paper.

1.1 To whom will the Act apply?

This paper recommends that the proposed Privacy Act should apply to "government bodies", as defined below. Government, of course, is not the only institution that holds and manages personal information, or whose activities can affect the personal privacy of individuals. In fact, in some ways the threats to individual privacy are more serious in the realm of private sector information management than in public sector information management. Private sector invasion of privacy issues include annoyances, such as uninvited telephone and mail solicitation, and more serious matters such as unauthorized use of an individual's transactional data (for example, debit and credit card data), and the compilation of personal profiles by the matching and linking of computerized data.

The possibility of applying privacy legislation in the private sector as well as the public sector is currently being examined elsewhere and is not dealt with in this paper. At present Quebec is the only Canadian jurisdiction with privacy legislation that applies to the private sector, but other jurisdictions are considering the matter. The federal government has begun a process of developing legislation for those areas of business under its jurisdiction, and has asked the Uniform Law Conference of Canada, on which New Brunswick is represented, to develop a model Act which could be uniformly adopted by provincial legislatures in relation to businesses under provincial jurisdiction. Since many private sector firms, and most of the large ones, operate in more than one province, this is clearly an area in which harmonization of provincial legislation is desirable. New Brunswick intends to participate in this project for developing common standards of privacy protection that will apply across the country. In the meantime, though, it sees no reason for delaying the implementation of privacy legislation in relation to provincial "government bodies".

The first task, then, is to define "government bodies" in a way that clearly identifies which agencies of government are to be subject to the Act. Other New Brunswick Acts that have to define "the government" often do so by means of a list established by regulation. It is thought that this approach will be appropriate for the Privacy Act. As for the content of the list, it is recommended that the starting point should be the list set out under the *Right to Information Act*. This is because of the various inter-connections between that Act and the Privacy Act that will be referred to in this paper. The existing list under the *Right to Information Act* is set out in Appendix A for information. However, the list under the Privacy Act should not necessarily be limited to the bodies to which the *Right to Information Act* applies. The Schedule under the

Privacy Act should be capable of expansion to include, eventually, all "government bodies" in a broad sense of the words.

Recommendation #1

It is recommended that the proposed Privacy Act should apply to all government bodies to which the *Right to Information Act* applies.

Recommendation #2

It is recommended that the proposed Privacy Act be capable of extension to other public sector organizations.

A relevant social trend is the increasing tendency of government to contract out to the private sector functions that were formerly provided by the public sector. Some of these functions involve the management of personal information. The privacy of New Brunswickers will only be fully ensured if the contracting company is obliged to take care of the personal information to the same degree that government would have been if it had been fulfilling the function.

Recommendation #3

It is recommended that where government bodies enter contracts under which private sector institutions will perform functions that involve the care or management of personal information for the government body, the privacy of the personal information must continue to be protected.

1.2 What is meant by "Personal Information"?

Only information that is "personal" falls within the ambit of a Privacy Act. A key question, then, is how "personal information" is defined. People have different views as to what sort of information about themselves they consider personal enough to be kept confidential, and this may depend on the circumstances. However, most information that can be tied to an identifiable individual will be considered "personal" by someone. To provide the broadest protection for the privacy of citizens, a Privacy Act should include a broad definition of "personal information", in which all information that can be tied to an identifiable individual is considered "personal".

Recommendation #4

It is recommended that "personal information" be defined as information about an identifiable individual recorded in any form.

Other Canadian privacy statutes, as well as the *Personal Privacy Code*, include a list of the kinds of things that are considered to be "personal information". Some examples from the *Code* are:

- information relating to race, national or ethnic origin, mother tongue, colour, creed, religion or political beliefs, age, sex, sexual orientation or marital status or family status;

- information that relates to health care that has been received by the individual or to the health history of the individual, including a physical, mental, psychiatric, or psychological disability;

- information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness, or which was obtained on a tax return or gathered for the purpose of tax collection;

- the name, home or business address, home or business telephone number, fingerprints, blood type or inheritable characteristics of the individual;

- the personal opinions or views of the individual . . . .

It may or may not prove useful, ultimately, to include a list of this sort in the Privacy Act. For present purposes, however, it is more important to appreciate the nature of the general definition than the specifics of the examples. Under the general definition any information is "personal" if it relates to an identifiable individual.

It is also important to appreciate the converse of this. Information, of whatever nature, is not "personal" information unless it relates to an identifiable individual, and information that is not "personal" will not be subjected to controls under the Act. Even information on matters such as race, religion, health or financial matters will be beyond the scope of the Act as long as there is no individual who can be personally associated with the information.

2 Collection of Personal Information

A government body's handling of personal information begins with the collection of that information. The first of the OECD principles, the "collection limitation principle", covers the nature of the information that a collecting institution can collect, and the manner in which the information may be collected.

2.1 Nature and manner of collection of information

It is a basic principle of fair information practices that an information-collecting agency should collect only such information as is required for the purpose for which it is collected. In the government context, this purpose will almost invariably be related to an existing or proposed program or function of the government body that does the collection. Enacting this principle into legislation will ensure that a government body does not come into possession of personal information that is "none of its business".

Recommendation #5

It is recommended that a government body be authorized to collect only such personal information as is required for the operation of an existing or proposed program or function of that government body.

Information can be acquired by a government body in one of three ways: it can be collected directly from the individual concerned, it can be disclosed to the government body by another government body, or it can be collected from a third party. The basic premise on which the OECD Guideline operates is that information should be collected directly from the person to whom it relates whenever possible. Collection from other sources would, of course, be permissible with the consent of the individual concerned. Other exceptions would need to be specified by law.

Recommendation #6

It is recommended that personal information should, whenever possible, be collected directly from the person to whom it relates, unless the individual authorizes otherwise or the collection is expressly authorized by law.

The principle of direct collection must co-exist with the current reality that governments are striving for efficiency and cost control. In many cases, it is both fair and reasonable for one government body to obtain information about a person from another government body. OECD Guidelines and Canadian privacy statutes permit government bodies to disclose personal information in a number of specified circumstances. This paper will be recommending similar rules on disclosure of personal information (see recommendations #17, #18 and #19). Where one government body is seeking information which is already in the possession of another government body, and the second body is permitted by the Privacy Act to disclose it, it is only natural that the first government body should be able to "collect" it from the second.

Recommendation #7

It is recommended that an exception to the principle in recommendation #6 be made to allow one government body to collect personal information from another government body when the Privacy Act permits disclosure by the second government body of the required information.

In other instances the collection of information from a private sector body or from another individual may be necessary. Sometimes, for example when the whereabouts of the person concerned are unknown, this would be permissible under recommendation #6, which only requires direct collection "whenever possible". In other cases, however, the person concerned may be available but there may be reason to believe that he or she, if asked directly, would not give accurate information. In such cases the individual might still be one source of the information, but other sources should also be available.

Recommendation #8

It is recommended that exceptions to the principle in recommendation #6 be made to allow a government body to collect personal information from sources other than the individual to whom the information relates in the following circumstances:

(a) when information is collected to assist in an investigation related to the enforcement of an Act or for the purpose of supervising an individual under the control of a correctional authority;

(b) when information is collected for the purpose of legal proceedings by the government body against the individual or for recovering a fine or debt owed to the government body;

(c) when information is collected for the purpose of determining an individual's suitability or eligibility for a program or benefit provided by the government body;

(d) when for any other reason collection from the individual directly might result in the collection of inaccurate information or prejudice the purpose for which the information is collected.

The next principle in the OECD Guidelines relating to the collection of personal information is the "purpose specification principle". This states that an information-collecting agency must identify the purpose for which the information is being collected. This purpose may be stated

very broadly, and may be as simple as the title on a form, e.g. "Driver's Licence Application". In other cases, it might be necessary to specify the purpose (or purposes) more precisely. This will have to be determined by the information collector depending on the circumstances.

Recommendation #9

It is recommended that a government body that collects personal information must identify the purpose for which the information is being collected.

In keeping with principles of openness in government activity, an information-collecting government body must also be prepared to take additional steps to reassure citizens about the validity and necessity of a collection of personal information. The more details an individual is given, the more comfortable he or she will be with giving a government body custody of his or her personal information. If the government official who is doing the collection is unfamiliar with these details, he or she should be able to offer the individual the name, address and telephone number of an official who can answer questions. At an electronic kiosk, it is especially important that the individual be given the means to receive further information and the name and telephone number of a contact person to whom they can direct their questions.

In addition to information about the purpose of the collection, government bodies must also be prepared to inform individuals of their rights under the Privacy Act, as described later in this paper, and to give them any further information they request as to the use that will be made of the information and the categories of persons who will have access to it.

Recommendation #10

It is recommended that, when collecting personal information, a government body must identify a contact person who will answer questions about the information collection and about the application of the proposed Privacy Act.

2.2 Accuracy of Information

Another principle of fair information practice is that the custodian of personal information must take reasonable steps to keep the information accurate, complete and up-to-date to the extent necessary for the purpose for which it was collected. What steps will be "reasonable" will vary in different circumstances, and in some cases the individual may also have a responsibility to keep his or her information current. Eventually, though, when the government body uses the information, it is the nature of the use that will determine what steps must be taken in accordance with the principle. If the government body will use the personal information to make a decision that directly affects the individual, it must do its best to ensure that the information

is accurate and complete. However, the principle allows for a somewhat lower standard of currency and accuracy if information is to be used only to plan government programs, or for statistical purposes.

Recommendation #11

It is recommended that a government body that holds personal information must take reasonable steps to ensure that the information is accurate and up-to-date to the extent necessary for the purpose for which it was collected or is to be used.

2.3 Protection of Information

It is obvious that the personal privacy of New Brunswickers will not be assured unless adequate security measures are taken to protect personal information that is within the custody of government. The knowledge that security measures will be strict is likely to add to people's comfort level and therefore to their level of compliance with government information collection. These security methods must ensure that personal information is secure against unauthorized access both from within and from outside government. Security methods must be appropriate both to the type of information and to the electronic or other form in which the information is held.

Recommendation #12

It is recommended that each government body must implement technical and organizational security measures to protect personal information against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure or access.

2.4 Retention and Destruction of Information

The destruction of personal information when it is no longer needed (unless it has historical value as determined by the Provincial Archivist) is essential to the proper management of information resources. The *Personal Privacy Code* of New Brunswick requires government to introduce and maintain the practice of routine destruction of information that is no longer needed and is not required for archival purposes. However, the personal information that has been used to make a decision about an individual must be kept long enough to allow the individual to have access to it to see for himself or herself upon what basis the decision was made.

Recommendation #13

It is recommended that if a government body uses personal information about an individual to make a decision about that individual or about a member of his or her family, the government body must retain the personal information for at least two years after the decision is made.

After a holding period, which may be longer than the period recommended above depending on the type of information and the purpose for which it was being used, all public records of the province can be transferred from the department where they reside to the Public Archives. The *Archives Act* provides that no public records (including those containing personal information) shall be destroyed or removed from the ownership and control of the Province unless such destruction or removal is authorized under that Act. The Provincial Archivist determines which records should be kept for historical purposes and authorizes the destruction of the other records according to a schedule.

Recommendation #14

It is recommended that the destruction of personal information in the control of a government body be governed by the *Archives Act*.

3 Use and Disclosure of Personal Information

3.1 Principle and Exceptions

One of the central principles of fair information practice is that personal information should be used or disclosed only for the purpose for which it was collected, or for a purpose consistent with that purpose, or with the individual's consent, or under a specified and publicly known exception. "Disclosure" in this context includes disclosure from one department to another within government, since each department is considered to be a separate "government body" for purposes of the Act.

Recommendation #15

It is recommended that personal information within the safekeeping of government be used or disclosed only for the purpose for which it was collected, or for a purpose consistent with that purpose, or with the individual's consent, or under an exception identified by the proposed Privacy Act.

"Consistent purpose" is defined in different Canadian privacy statutes either as something that is directly related to the original purpose or as something that is within the reasonable expectations of the individual whose information is in question. It is thought that the concept of an individual's "reasonable expectations" comes closer to capturing those situations in which the average citizen would not object if his or her personal information is used without his or her direct consent.

Recommendation #16

It is recommended that "consistent purpose" be defined as a purpose for which an individual who had provided information to a government body would reasonably expect that the information might be used or disclosed.

The decision as to whether a purpose is consistent or not would be made by the head of the government body that proposed to use or disclose the information. This decision should be an objective one, focusing on the relationship between the original purpose and the potentially "consistent" one, and is, in principle, a decision that should hold good for all cases, not just for the specific case in which the decision is taken. For this reason Canadian privacy statutes normally require the head of the government body to ensure that, where a use of information is found to be "consistent with" the different purpose for which the information was originally collected, the "consistent purpose" is publicly identified. The directory of personal information (see recommendation #27) is normally the place where this identification occurs.

There are a number of other situations in which Canadian privacy statutes typically permit the use or disclosure of personal information even though for purposes other than those for which it was originally collected. In some of these situations the disclosure is for the benefit of the individual. In other cases the disclosure relates to matters such as law enforcement, public health and safety, or eligibility for government benefits, where the broader interests of society outweigh the individual's possible preference for information about himself or herself to be kept confidential within a particular government body. In the case of determining an individual's suitability or eligibility for a government program or benefit, individuals will generally be informed when they apply that the information they provide may be confirmed with other sources.

Another special case exists where disclosures are expressly authorized by other New Brunswick Acts. A general statute like the Privacy Act cannot contemplate every situation in which a government body may have valid reasons to use or disclose particular kinds of personal information without the consent of the individual. Such situations are sometimes directly addressed in other statutes. In accordance with the OECD principle that uses that are provided for by law should be permitted, other statutes will continue to be able to make special provisions for special situations. They will also, of course, be able to impose stricter controls on the use

or disclosure of particular kinds of personal information if, in specific contexts, added protection beyond the general rules in the Privacy Act is felt to be required.

Recommendation #17

It is recommended that a government body should also be able to use or disclose personal information in the following circumstances:

(a) for the purpose of complying with an order of a court or other body having authority to compel disclosure;

(b) to assist another government body or a federal agency in an investigation related to the enforcement of an Act;

(c) to assist in the enforcement of a maintenance or support order;

(d) for the purpose of supervising an individual under the control of a correctional authority;

(e) for use in a court or tribunal in proceedings involving the government of New Brunswick;

(f) for the purpose of collecting a fine or debt owing by an individual to a government body or of making a payment owed by a government body to an individual;

(g) for the purpose of determining an individual's suitability or eligibility for a program or benefit provided by the government of New Brunswick or the federal government;

(h) so that the next of kin or a friend of an injured, ill or deceased person may be contacted;

(i) where necessary to protect the mental or physical health or safety of an individual or to protect the public health or safety;

(j) for research or statistical purposes, provided that the privacy of the individual can be adequately protected, or for historical preservation as prescribed by the *Archives Act*;

(k) when a substantial public interest or a benefit to the individual clearly outweighs the invasion of privacy that could result from the disclosure;

(l) in accordance with any Act of New Brunswick or Canada that authorizes or requires such use or disclosure.

There are also some kinds of information that, though "personal", are of legitimate public interest, and should be disclosable without needing to fit into any of the circumstances above. Some of these items may in fact be things to which the public has or should have a right of access under the *Right to Information Act*, but that is an issue beyond the scope of this paper. So far as the proposed Privacy Act is concerned, the most that should be said here is that nothing in the Privacy Act should prevent a government body from disclosing the information listed below.

Recommendation #18

It is recommended that nothing in the Privacy Act should prevent a government body from disclosing

(a) the classification, salary or salary range, benefits and employment responsibilities of an individual who is or was an officer or employee of a government body;

(b) expenses incurred by an individual travelling at the expense of a government body;

(c) the advice and opinions of an individual employed by a government body given in the course of employment;

(d) information about the terms of contracts entered into by individuals with a government body and the performance of their contractual obligations;

(e) details of a licence, permit or other similar discretionary benefit granted to an individual by a government body;

(f) details of a financial benefit of a discretionary nature granted to an individual by a government body.

The fact that a government body had authority to disclose information under recommendation #17 or #18 would not mean that disclosure would always be appropriate. A balancing of the interests involved would normally be required, leading to a determination of whether, in the circumstances, a disclosure of personal information would be an unreasonable invasion of the privacy of the individual. The Privacy Act should describe the general nature of the balancing that should be carried out.

Recommendation #19

It is recommended that personal information should only be used or disclosed under recommendations #17 or #18 where the use or disclosure would not amount to an unreasonable invasion of privacy, taking into account the specific nature of the personal information and the specific purpose for which it is to be used or disclosed.

In a different context, that of situations in which governments have to decide whether to release personal information in response to applications under access to information legislation, the statutes of several provinces have attempted to give substance to the idea of an "unreasonable invasion of privacy". The approach has been a flexible one, creating a presumption that disclosure of things such as health or tax records or information about a person's racial or ethnic origins or political or religious beliefs will normally be an "unreasonable invasion of privacy", but putting this within the context of a broader requirement to consider all of the relevant circumstances in deciding whether information should be released. This approach may well be useful in the present context also.

4 Right of Access to One's Own Personal Information

4.1 Right of Access

It is a basic principle of privacy protection that an individual about whom information has been collected should have a right of access to that information in an intelligible form, either to view it or to receive copies. An individual may desire access simply to satisfy his or her own curiosity, or to determine on what basis the government has made or will make a decision relating to him or her, or to verify the accuracy of the information. A right of access to one's own personal information is found in the OECD Guidelines, in other Canadian privacy statutes, and in the EU Directive. Such a right also exists under the *Right to Information Act*, but that Act is not designed with access to one's own personal information primarily in mind, and is consequently not well adapted for the purposes under consideration here.

International principles of fair information practice recognize that there is a cost involved in providing access for individuals to their own personal information, and that it is acceptable to pass some of that cost on to the individual by the application of a reasonable fee. The fee may recover the cost of the retrieval and copying of documents, provided that cost is not prohibitive. Fees should not be used to discourage access by individuals to their own personal information.

Recommendation #20

It is recommended that an individual have a right of access to his or her own personal information in an intelligible form, in the language in which it occurs in the government body's storage system, and for a reasonable fee.

There are several circumstances, however, in which it may be appropriate to deny an individual access to his or her personal information. These include when serious harm may result to the applicant or another individual by virtue of such access, when the information has been gathered for the purpose of law enforcement, when the information has been supplied in confidence (such as employment references, evaluation of test scores and other confidential assessments), or when the individual's personal information is so inextricably linked with the personal information of another individual that its disclosure to the first individual would result in a violation of the privacy of the second individual.

Recommendation #21

It is recommended that exceptions to the individual's right of access to his or her personal information should be allowed in the following circumstances:

(a) where serious harm would result to the applicant or to another individual if the applicant were given access;

(b) where the personal information was gathered for the purpose of law enforcement or where its disclosure would impede an investigation, an inquiry or the administration of justice, or be harmful to the public safety or security;

(c) where the information was provided to the government body, explicitly or implicitly, in confidence;

(d) where the information requested is inextricably linked to the personal information of a third person;

(e) where the information is subject to any sort of legal privilege, including solicitor-client privilege.

Where one of these exceptions applied, there would be no right of access, but the head of the government body would still be required to determine whether, as a matter of discretion, the information should be released to the individual. In some cases this could be done by deleting from a document material that fell within the exceptions above, and releasing the remainder of

the document. In other cases a decision would have to be made about whether in the specific circumstances the individual's need to know the information prevailed over the public or private interest that the exception was devised to protect. In the case of item (c), in particular (information provided in confidence), it would sometimes be appropriate to require a government body to provide a summary of the information in its possession, even if the information itself should not be released. Without having even a summary of the information in the government body's possession the individual might be completely unaware of the basis on which decisions affecting him or her were being taken.

4.2 Procedure

Under the *Right to Information Act*, any person may request information by applying to the head of the government body where the information is likely to be kept. The applicant must, as far as possible, specify the document or documents in which the relevant information is likely to be found. Current practice is that each head of a government body has delegated a person to look after *Right to Information Act* requests. The same procedure should be used for an access or correction request under the proposed Privacy Act. The head of a government body should have the power to delegate the function of responding to privacy requests (perhaps to the same person who currently fulfils this function for *Right to Information Act* requests).

Recommendation #22

It is recommended that the same procedure should apply to access to personal information under the proposed Privacy Act as applies to access to general information under the *Right to Information Act*.

The time limit during which a Minister must reply to a request for access to information under the present *Right to Information Act* is 30 days. Although it is recognized that even 30 days is a long time for a person to wait for a reply, for some complicated requests this time period is considered inadequate by the people who must respond to the requests. The Privacy Act should provide for the initial 30 day period to be extended, although not by more than an additional 30 days.

Recommendation #23

It is recommended that a time limit of 30 days be imposed upon the head of a government body to respond to a request for access to personal information, but that an extension of 30 days should be available if it is impossible to respond to the request within the initial 30 day period.

4.3 Right to request correction

If a government body inadvertently uses incorrect personal information to make a decision about an individual, this can have serious consequences for that individual. It can decrease or eliminate an individual's eligibility for social programs or benefits, or be harmful to the individual in other ways. Thus it is vital that, in addition to the right of access, an individual should have the right to request correction of his or her personal information if he or she believes the information is inaccurate. A request for a correction would sometimes arise out of a formal access request that revealed information that the individual believed to be inaccurate. However, the individual should also be able to request a correction independently of an access request.

In some instances a difference in opinion may occur between the individual and the government body as to whether the individual's personal information is accurate. If the individual can demonstrate to the satisfaction of the head of the government body that the information is inaccurate, the requested correction should be made. If the individual cannot demonstrate the inaccuracy to the head's satisfaction, the head should be obliged to attach an annotation to the information stating the nature of the correction requested and the reason it was not made.

Recommendation #24

It is recommended that an individual be entitled to request corrections to his or her personal information, and to have inaccurate information corrected.

Recommendation #25

It is recommended that, if a government body declines to make a correction, the government body must put an annotation on the information reflecting the nature of the individual's request, the fact that the request was denied and the reason for the denial.

In many cases requests for correction would be dealt with on an informal basis in the course of dealings between the government body and the individual. However, there should also be a formal process designed to ensure that disagreements between a government body and an individual can be brought to a conclusion. When a formal request for correction is made, the same time limits should apply as on a request for access to personal information.

To have full meaning, the right to receive a correction or annotation to one's personal information must extend past the government body to whom the correction request is directed, out to third parties (including other government bodies) to whom the original government body may have disclosed the information as allowed under the proposed Privacy Act. This means that

a government body has a responsibility to inform third parties to whom the information has been disclosed of any correction or annotation that has been made to the information. Not only will the individual benefit from such a system by knowing that the correction or annotation has been communicated to other bodies in possession of the personal information, but the system will help the other bodies fulfil their obligation to keep their information accurate and up-to-date.

The requirement to notify other bodies, however, must be subject to reasonable limitations. For example, several recent privacy Acts from other provinces provide that corrections or annotations only need to be passed on to bodies to whom the incorrect information has been disclosed within the previous year. It is also possible that in establishing the level of obligation to be imposed on government bodies in this regard, the seriousness of the error and its possible consequences may be factors to be considered.

Recommendation #26

It is recommended that a government body be subject to a reasonable requirement to communicate to third parties any correction of or annotation to personal information that the government body has previously disclosed to the third party.

4.4 Directory

Under the *Right to Information Act*, an individual is required to direct his or her request for access to personal information to the government body that holds the information. The same procedure is proposed for the Privacy Act (see recommendation #22). However, the citizen will have great difficulty exercising his or her rights unless he or she has some way of knowing which government bodies may hold such information. To assist the citizen in making this determination, other Canadian jurisdictions with privacy and access legislation have required their governments to publish a directory of information held by government bodies. In the case of personal information, such a directory typically includes a list of the type of information each government body holds, the purpose for which it was collected and is being used, and the categories of persons within or beyond that body who have access to the personal information.

Recommendation #27

It is recommended that the Government of New Brunswick develop a personal information directory, listing the names and addresses of government bodies that hold personal information, the type of information each holds, the purpose for which that information was collected and is being used, and the categories of persons who have access to that information.

The directory should be developed with the ease of the user in mind. It should take advantage of information technology, and might not need to be produced in a printed form at all. The possibility of access to the directory through an organization such as Service New Brunswick should be considered, with a view to simplifying the process as much as possible from the point of view of the individual user.

5 Supervision, Review and Appeal

5.1 Supervisory Authority

The appointment of an independent supervisory authority is the method by which most jurisdictions have chosen to ensure the optimum functioning of their legislated privacy schemes. The EU Directive of 1995, discussed in the Introduction to this paper, provides that each member country must appoint an independent supervisory authority. Canadian jurisdictions, with the exception of Nova Scotia, have established an office of the Privacy Commissioner, or in Quebec a multi-member Commission, to fulfil the role of supervisory authority. For the federal government, the Privacy Commissioner only deals with privacy matters. In the provinces the Commission or Commissioner also has responsibilities in relation to access to information, since the relevant statutes combine privacy protection and access to information within a single Act.

The beneficial services that could be performed by a supervisory authority include receiving and investigating complaints from citizens and reviewing the personal information management practices of government departments to ensure that these comply with the privacy principles of the proposed Act.

Recommendation #28

It is recommended that a supervisory authority be appointed to fulfil the functions assigned to it by the proposed Privacy Act.

In New Brunswick the most suitable body to perform the functions of supervisory authority is the Office of the Ombudsman. This office already functions to investigate complaints about matters of administration and to make more systematic investigations of government practices. The Office of the Ombudsman was given responsibility for supervising and investigating complaints relating to the *Personal Privacy Code*, and already has responsibilities in relation to complaints of wrongful denial of access under the *Right to Information Act*. It has developed an expertise in these related areas, and has the administrative structure to cope with an expanded role. The Ombudsman is appointed on the recommendation of the Legislative Assembly and reports to the Legislative Assembly, thus maintaining the independence that is important to the functioning of the supervisory authority.

Recommendation #29

It is recommended that the role of supervisory authority of the proposed Privacy Act be placed with the Office of the Ombudsman.

5.2 Powers of the Supervisory Authority

The role of a supervisory authority can be divided into two main components:

1. the investigatory and complaint resolution functions;
2. the review, advice-giving, research, and public education functions.

In EU member countries, in the provinces where a Commission or a Commissioner exists and at the federal level, the responsibilities of the supervisory authority encompass both these areas. The first component area, the investigatory and complaint-resolution functions, benefits citizens by providing a mode of redress for real or perceived violations of the privacy principles enunciated in the Act. The second component area, the review, advice-giving, research and public education functions, benefits both government and citizens by promoting adherence by government bodies to the privacy principles enunciated above.

Recommendation #30

It is recommended that the functions of the Ombudsman as the supervisory authority for the proposed Privacy Act be as follows:

(a) to receive complaints about the operation of the proposed Privacy Act;

(b) to conduct investigations, either on her own initiative or upon request, and to recommend resolutions for the complaints received;

(c) to conduct research and public education into issues of personal privacy;

(d) to review and comment on the privacy implications of legislative or administrative schemes or programs and their compliance with the proposed Privacy Act;

(e) to give advice and recommendations of general application to the head of a public body on matters respecting the rights or obligations of a head under the Act.

With regard to the investigatory and complaint-resolution functions, other Canadian jurisdictions illustrate two models of supervisory authority. These are the supervisory authority with the power to make orders to government bodies (B.C., Alberta, Ontario, Quebec) and the supervisory authority without such order powers (Saskatchewan and the federal government).

Under the first model, the supervisory authority investigates a citizen's complaint and may ultimately make an order to the government body concerned. The government body must comply with the order or else appeal to the courts. Under the second model, the supervisory authority makes recommendations, rather than orders, and a more flexible relationship between the supervisory authority and the government body prevails until a satisfactory resolution is reached.

At present under New Brunswick's *Ombudsman Act* the Ombudsman is a form of supervisory authority without order powers. The advantage of that model is that it is conducive to co-operation in problem-solving, and experience under that Act has been that, through the process of recommendation and persuasion, the Ombudsman has almost invariably been able to bring government bodies to provide the remedies that the Ombudsman believes to be appropriate. It is thought that this sort of flexible relationship between the supervisory authority and government bodies would be a positive influence on the Privacy Act, and that it is therefore preferable that order powers should not be included in the Act.

5.3 Investigations

If the Ombudsman is to be the supervisory authority under the Privacy Act, it would be natural that her investigatory powers be the ones set out in the *Ombudsman Act*. These do indeed appear to be suitable for the task. The *Ombudsman Act* provides that all investigations shall be conducted in private, that the Ombudsman may obtain information from any person, may make inquiries, may summon and examine any person upon oath, and may regulate her own procedure.

Recommendation #31

It is recommended that the supervisory authority have powers of investigation as provided under the *Ombudsman Act*.

5.4 Dispute Resolution and Appeal

The Privacy Act proposed in this paper contains two kinds of provisions. There are rules of conduct applying to the collection, handling, use and disclosure of personal information by government bodies; there is also the individual's right of access to his or her own personal

information. As noted previously, a comparable right of access exists at present under the *Right to Information Act*.

It is thought that the dispute resolution and appeal mechanisms of the proposed Privacy Act should reflect these different elements of the Act. It has been recommended above that the Ombudsman should act as the supervisory authority for the Act, and that the Ombudsman's normal power of recommendation should be adequate to ensure satisfactory compliance with the Act. The power is a very flexible one. It can be used to attain whatever the Ombudsman considers to be the appropriate remedy in a specific situation, and this may, in an appropriate case, include financial compensation. This flexible approach seems well suited to resolving the variety of complaints that may arise about the collection, handling, use or disclosure of personal information.

In relation to access to one's own personal information, however, a different situation prevails. In this case the individual has a right to obtain the information, and the remedies should be comparable to those provided under the *Right to Information Act*. Under that Act, an aggrieved individual, after his or her request for information has been refused by the head of a government body, has the choice of proceeding to court or proceeding to the Ombudsman. The court can order the disclosure of information. The Ombudsman, by contrast, still only has her normal power to make recommendations to a government body for the release of information, but if the government body does not follow the Ombudsman's recommendation, the complainant can appeal to the court.

Recommendation #32

It is recommended that

(a) in the case of a wrongful refusal of access to personal information under the proposed Privacy Act the individual's remedies should be the same as the remedies for wrongful refusal of access to other information under the *Right to Information Act*;

(b) for other complaints under the proposed Privacy Act the Ombudsman's powers under the *Ombudsman Act* should be the means of redress.

6 Internal Administration

Formal authority for the administration of the Privacy Act in a government body will be given to the deputy head or other chief executive officer. For the smooth and consistent operation of the legislation, however, an official in the government body should also be designated to co-ordinate activities under the Act. In very small agencies this might perhaps be the deputy head in person. More often, though, he or she would appoint someone else.

Recommendation #33

It is recommended that in each government body a person be designated to be responsible for the operation of the Privacy Act.

To ensure consistency between the practices of different government bodies, it may also be desirable to establish a small advisory committee. This would be particularly useful during the early stages of the implementation of the Act, when deputy heads and designated privacy co-ordinators would be dealing with unfamiliar issues, but it might also be useful on a continuing basis. Decisions on issues such as "consistent purposes" and "unreasonable invasion of privacy" may not always be straightforward, and it may be useful in the long term as well as in the short term to have an internal focus of expertise to which government bodies can turn in cases of uncertainty.

It would probably not be necessary for this committee to be established on a statutory basis. Its role would be essentially consultative, with formal internal decision-making authority under the Act remaining with the heads of government bodies. Nonetheless the committee's role would be an important one. Consistency in the application and interpretation of the Act, with a proper awareness of its objectives, is something that the government must strive to attain. Achieving this would be the essence of the committee's functions.

Recommendation #34

It is recommended that a committee be established to give advice to deputy heads and privacy co-ordinators as to the implementation and administration of the proposed Privacy Act. This committee should operate for at least an initial period after the Act is proclaimed.

7 Offences and Penalties

Offences and penalties in an Act provide a method of ensuring compliance with key elements of the statutory scheme. They also serve the purpose of pointing out that violations of the Act will be viewed seriously.

It is a general principle of law that no-one should be punished unless he or she is at fault. The general standard of fault in the privacy statutes of other Canadian jurisdictions is that the head of the government body or his or her delegate will only be liable to be prosecuted and fined under the Act if they have "wilfully" or "knowingly" violated the Act. An official whose conduct does not meet this standard but who is nonetheless guilty of a misconduct in relation to the Privacy Act should be dealt with through internal disciplinary measures. Disciplinary

measures could also be taken, of course, against people who had committed offences under the Act; in their case the disciplinary measures would be cumulative with the prosecution.

Recommendation #35

It is recommended that an official of a government body who wilfully collects, uses, discloses or withholds personal information in violation of the proposed Privacy Act, or who destroys any records with the intent to evade a request for access to the records, commits an offence and is liable to a fine.

There are two other ways in which the operation of the proposed Privacy Act could be impeded: through obstruction of the Ombudsman's investigations and through applications for personal information made under false pretences. The proposed Privacy Act should make it clear that such actions will not be tolerated.

Recommendation #36

It is recommended that any person who, without lawful justification, obstructs or misleads the Ombudsman, or any person who applies for or requests access to or correction of personal information under false pretences, commits an offence and is liable to a fine.

8 Regulation-Making Power

Some aspects of a privacy scheme can more effectively be placed under the regulation-making power of the Lieutenant-Governor in Council than directly in the legislation. These include especially those aspects of the legislative scheme that may require frequent additions, such as a list of the government bodies to which the Act applies or a list of those persons who are designated as heads of government bodies under the Act. There may also be some procedural matters that it is more appropriate to establish by regulation than in the Act.

Recommendation #37

It is recommended that the proposed Privacy Act contain regulation-making power to cover the following matters:

(a) prescribing a list of departments, boards, commissions and other bodies that are to be considered "government bodies" for the purposes of the Act;

(b) prescribing a list of persons to be considered heads of government bodies for the purposes of the Act;

(c) respecting the procedure to be followed on an application for access or a request for correction of personal information, or respecting the procedure to be followed in making a complaint to the Ombudsman;

(d) prescribing the amount of fees and respecting the circumstances under which a head can waive a fee;

(e) respecting forms for use under the Act.

9 Transitional and Consequential

There are many New Brunswick Acts that deal with the collection, handling and disclosure of information, and some of that information is personal information within the meaning of the proposed Privacy Act. In some cases there are differences between the treatment that the information receives under another Act and the treatment it would receive if the proposed Privacy Act were the only applicable legislation. For example, other Acts may sometimes allow disclosure of information when the Privacy Act would not, and sometimes they may oblige a government body to keep information confidential when the Privacy Act would permit its disclosure. Other, less clear-cut, forms of inter-relationship between the Privacy Act and other Acts are also possible.

In the preparations for the implementation of the Privacy Act, government bodies should attempt to identify areas of conflict between the Privacy Act and other Acts for which they are responsible, and should promote amendments to the other Acts where appropriate. There will be cases, of course, in which no amendment to the other Act should be made; in some instances there will be very good reasons why a particular kind of information is to be treated in the way prescribed in the other Act -- for example by being given additional protection beyond what the Privacy Act would provide. Nonetheless, where amendments are appropriate, it would be beneficial to deal with them as a package of consequential amendments accompanying the Privacy Act.

One Act, however, which will certainly need amending and which deserves special attention here is the *Right to Information Act*. That Act currently allows for access requests by an individual relating to his or her own personal information, a subject that this paper has described as being suitable for inclusion in the Privacy Act. This right of access should not be dealt with under both Acts. There are two other obvious points at which the Privacy Act and the *Right to Information Act* would connect. One is where an access request under the *Right to Information Act* produces personal information about a third party, thus raising the question of whether the personal information should or should not be disclosed. The other is where an individual requests his or her own personal information under the Privacy Act, but disclosure of that

information would reveal information that is protected under the *Right to Information Act*, for example trade secrets or Cabinet confidences.

The first of these issues is whether the individual's right of access to his or her own personal information should be placed in the Privacy Act or the *Right to Information Act*. This issue would not arise, of course, if the Privacy Act and the *Right to Information Act* were combined into a single Act, as a number of provinces (but not the federal government) have done. However, on the assumption that the two Acts are to remain separate, it is thought that the Privacy Act is the more appropriate location and that the *Right to Information Act* should be amended accordingly.

Recommendation #38

It is recommended that the *Right to Information Act* be amended to provide that the relationship of an individual to a government body vis-à-vis his or her own personal information, including access to that information, is governed by the proposed Privacy Act and not by the *Right to Information Act*.

The next issue relates to cases in which a release of information on an ordinary access request under the *Right to Information Act* would reveal personal information about a third party. The *Right to Information Act* provides that the applicant has no right to the information in these cases, but it leaves the head of the government body a discretion to release the information. However, it provides no criteria on which the exercise of that discretion is to be based. It is thought that the provisions of the Privacy Act relating to disclosure of personal information should be the key to whether personal information would be released on an application under the *Right to Information Act*. In accordance with recommendation #19, the critical decision here would be whether the release of the information would be an unreasonable invasion of privacy.

Recommendation #39

It is recommended that section 6 of the *Right to Information Act* be amended to link the disclosure of third party personal information under that Act to the disclosure provisions of the proposed Privacy Act.

As for the question of access requests under the Privacy Act that would reveal information that is protected from disclosure under the *Right to Information Act*, the starting point should be that where information is protected under the *Right to Information Act* the individual should not have the right to see it on an application under the Privacy Act. Again, though, the information might be made available on a discretionary basis, and this raises once more the question of how

government bodies should exercise their discretion to release information that they are not obliged to release. Here it becomes hard to make specific recommendations; there are too many kinds of potentially conflicting interests involved in the various categories of protected information referred to in the *Right to Information Act*. What can be said in general terms, though, is that when a government body is deciding how to exercise its discretion to release or not to release personal information that is protected from disclosure on some other ground under the *Right to Information Act*, it should place considerable importance on the individual's right to know the information that the government possesses about him or her.

A further major point of discrepancy between the *Right to Information Act* and the proposed Privacy Act relates to the definition of "personal information". The *Right to Information Act*'s definition lists types of information that are to be considered "personal"; the recommendation for the Privacy Act, by contrast, is that any information should be considered to be "personal" if it is about an identifiable individual.

In order for the two Acts to work together, the two definitions must match. On the basis of the present definitions, for example, some of the information that is to receive special protection under the Privacy Act would be accessible to third parties under the more limited definition of personal information currently found in the *Right to Information Act*.

Recommendation #40

It is recommended that the definition of "personal information" in the *Right to Information Act* be amended to match the definition of personal information proposed in recommendation #4.

Comparable amendments will be needed in the *Archives Act*. That Act contains a set of provisions that interact with the *Right to Information Act*, and are designed to ensure that a proper balance between public access to documents and the confidentiality of certain kinds of information is preserved even after the material is transferred to the archives. The *Archives Act* contains the same definition of "personal information" as the *Right to Information Act*, and states that records that would reveal personal information concerning another person are not available for public inspection until one hundred years after the date of that person's birth. During that period, however, access to the personal information can be allowed for the purpose of legitimate research or statistical work if the work cannot reasonably be accomplished without inspection of the record and an undertaking of confidentiality is given, in the form prescribed by regulation. Breach of the undertaking is an offence.

In order to ensure consistency with the *Right to Information Act* and the proposed Privacy Act, the *Archives Act* will need to be amended. The amendments should be based on the standard definition of "personal information" recommended for the other two Acts and on their proposed common approach to using the criterion of an "unreasonable invasion of privacy" in

determinations of whether or not personal information should be disclosed. Starting from this base, special provisions will need to be made in the *Archives Act* to strike the right balance between general privacy requirements and the desirability of public availability of archival material. The reason for preserving material in the archives is that it is of potential value to researchers and to posterity, and, as is exemplified by the present hundred year rule and the research exception in the *Archives Act*, over-protection of personal information under the *Archives Act* could undermine the very purpose for which the archives exist.

Recommendation #41

It is recommended that the *Archives Act* be amended to ensure that personal information is dealt with under that Act in a manner that is consistent with the *Right to Information Act* and the proposed Privacy Act, but which recognizes the special considerations that apply in relation to archival material.

The *Right to Information Act* and the *Archives Act* are, along with the proposed Privacy Act, the principal general statutes bearing on the government's handling of personal information. The inter-connecting package of amendments described in this paper should ensure that individual privacy is properly protected at all stages of the existence of that information, from its original collection, through its use, to its destruction or, in suitable cases, to its continuing availability as part of the historic record of the province of New Brunswick.

APPENDIX A -- LIST OF GOVERNMENT BODIES

(Schedule A to N.B. Reg. 85-68 under the *Right to Information Act*)

Advisory Council on the Status of Women

Board of Commissioners of Public Utilities

The Board of the New Brunswick Museum

Le Centre Communautaire Sainte-Anne

Department of Advanced Education and Labour

Department of Agriculture and Rural Development

Department of Economic Development and Tourism

Department of Education

Department of the Environment

Department of Finance

Department of Fisheries and Aquaculture

Department of Health and Community Services

Department of Human Resources Development

Department of Intergovernmental Affairs

Department of Justice

Department of Municipalities, Culture and Housing

Department of Natural Resources and Energy

Department of the Solicitor General

Department of Supply and Services

Department of Transportation

Executive Council Office

Fort LaTour Development Authority

Kings Landing Corporation

Labour and Employment Board

Legislative Library

Lotteries Commission of New Brunswick

Military Compound Board

New Brunswick Emergency Measures Organization

New Brunswick Film Classification Board

New Brunswick Fisheries Development Board

New Brunswick Geographic Information Corporation

New Brunswick Highway Corporation

New Brunswick Housing Corporation

New Brunswick Industrial Development Appeal Board

New Brunswick Industrial Development Board

New Brunswick Investment Management Corporation

New Brunswick Liquor Corporation

New Brunswick Power Corporation

New Brunswick Research and Productivity Council

New Brunswick Transportation Authority

Office of the Attorney General

Office of the Auditor General

Office of the Premier

Premier's Council on the Status of Disabled Persons

Region 1 Hospital Corporation (South-East)/Corporation hospitalière de la Région 1 (sud-est)

Region 1 Hospital Corporation (Beauséjour)/Corporation hospitalière de la Région 1 (Beauséjour)

Region 2 Hospital Corporation/Corporation hospitalière de la Région 2

Region 3 Hospital Corporation/Corporation hospitalière de la Région 3

Region 4 Hospital Corporation/Corporation hospitalière de la Région 4

Region 5 Hospital Corporation/Corporation hospitalière de la Région 5

Region 6 Hospital Corporation/Corporation hospitalière de la Région 6

Region 7 Hospital Corporation/Corporation hospitalière de la Région 7

Regional Development Corporation

Regional Family Income Security Appeal Boards

APPENDIX B -- SUMMARY OF RECOMMENDATIONS

1.1 To whom will the Act apply?

Recommendation #1

It is recommended that the proposed Privacy Act should apply to all government bodies to which the *Right to Information Act* applies.

Recommendation #2

It is recommended that the proposed Privacy Act be capable of extension to other public sector organizations.

Recommendation #3

It is recommended that where government bodies enter contracts under which private sector institutions will perform functions that involve the care or management of personal information for the government body, the privacy of the personal information must continue to be protected.

1.2 What is meant by "Personal Information"?

Recommendation #4

It is recommended that "personal information" be defined as information about an identifiable individual recorded in any form.

2.1 Nature and manner of collection of information

Recommendation #5

It is recommended that a government body be authorized to collect only such personal information as is required for the operation of an existing or proposed program or function of that government body.

Recommendation #6

It is recommended that personal information should, whenever possible, be collected directly from the person to whom it relates, unless the individual authorizes otherwise or the collection is expressly authorized by law.

Recommendation #7

It is recommended that an exception to the principle in recommendation #6 be made to allow one government body to collect personal information from another government body when the Privacy Act permits disclosure by the second government body of the required information.

Recommendation #8

It is recommended that exceptions to the principle in recommendation #6 be made to allow a government body to collect personal information from sources other than the individual to whom the information relates in the following circumstances:

(a) when information is collected to assist in an investigation related to the enforcement of an Act or for the purpose of supervising an individual under the control of a correctional authority;

(b) when information is collected for the purpose of legal proceedings by the government body against the individual or for recovering a fine or debt owed to the government body;

(c) when information is collected for the purpose of determining an individual's suitability or eligibility for a program or benefit provided by the government body;

(d) when for any other reason collection from the individual directly might result in the collection of inaccurate information or prejudice the purpose for which the information is collected.

Recommendation #9

It is recommended that a government body that collects personal information must identify the purpose for which the information is being collected.

Recommendation #10

It is recommended that, when collecting personal information, a government body must identify a contact person who will answer questions about the information collection and about the application of the proposed Privacy Act.

2.2 Accuracy of Information

Recommendation #11

It is recommended that a government body that holds personal information must take reasonable steps to ensure that the information is accurate and up-to-date to the extent necessary for the purpose for which it was collected or is to be used.

2.3 Protection of Information

Recommendation #12

It is recommended that each government body must implement technical and organizational security measures to protect personal information against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure or access.

2.4 Retention and Destruction of Information

Recommendation #13

It is recommended that if a government body uses personal information about an individual to make a decision about that individual or about a member of his or her family, the government body must retain the personal information for at least two years after the decision is made.

Recommendation #14

It is recommended that the destruction of personal information in the control of a government body be governed by the *Archives Act*.

3 Use and Disclosure of Personal Information

Recommendation #15

It is recommended that personal information within the safekeeping of government be used or disclosed only for the purpose for which it was collected, or for a purpose consistent with that purpose, or with the

individual's consent, or under an exception identified by the proposed Privacy Act.

Recommendation #16

It is recommended that "consistent purpose" be defined as a purpose for which an individual who had provided information to a government body would reasonably expect that the information might be used or disclosed.

Recommendation #17

It is recommended that a government body should also be able to use or disclose personal information in the following circumstances:

(a) for the purpose of complying with an order of a court or other body having authority to compel disclosure;

(b) to assist another government body or a federal agency in an investigation related to the enforcement of an Act;

(c) to assist in the enforcement of a maintenance or support order;

(d) for the purpose of supervising an individual under the control of a correctional authority;

(e) for use in a court or tribunal in proceedings involving the government of New Brunswick;

(f) for the purpose of collecting a fine or debt owing by an individual to a government body or of making a payment owed by a government body to an individual;

(g) for the purpose of determining an individual's suitability or eligibility for a program or benefit provided by the government of New Brunswick or the federal government;

(h) so that the next of kin or a friend of an injured, ill or deceased person may be contacted;

(i) where necessary to protect the mental or physical health or safety of an individual or to protect the public health or safety;

(j) for research or statistical purposes, provided that the privacy of the individual can be adequately protected, or for historical preservation as prescribed by the *Archives Act*;

(k) when a substantial public interest or a benefit to the individual clearly outweighs the invasion of privacy that could result from the disclosure;

(l) in accordance with any Act of New Brunswick or Canada that authorizes or requires such use or disclosure.

Recommendation #18

It is recommended that nothing in the Privacy Act should prevent a government body from disclosing

(a) the classification, salary or salary range, benefits and employment responsibilities of an individual who is or was an officer or employee of a government body;

(b) expenses incurred by an individual travelling at the expense of a government body;

(c) the advice and opinions of an individual employed by a government body given in the course of employment;

(d) information about the terms of contracts entered into by individuals with a government body and the performance of their contractual obligations;

(e) details of a licence, permit or other similar discretionary benefit granted to an individual by a government body;

(f) details of a financial benefit of a discretionary nature granted to an individual by a government body.

Recommendation #19

It is recommended that personal information should only be used or disclosed under recommendations #17 or #18 where the use or disclosure would not amount to an unreasonable invasion of privacy, taking into account the specific nature of the personal information and the specific purpose for which it is to be used or disclosed.

4 Right of Access to One's Own Personal Information

Recommendation #20

It is recommended that an individual have a right of access to his or her own personal information in an intelligible form, in the language in which it occurs in the government body's storage system, and for a reasonable fee.

Recommendation #21

It is recommended that exceptions to the individual's right of access to his or her personal information should be allowed in the following circumstances:

(a) where serious harm would result to the applicant or to another individual if the applicant were given access;

(b) where the personal information was gathered for the purpose of law enforcement or where its disclosure would impede an investigation, an inquiry or the administration of justice, or be harmful to the public safety or security;

(c) where the information was provided to the government body, explicitly or implicitly, in confidence;

(d) where the information requested is inextricably linked to the personal information of a third person;

(e) where the information is subject to any sort of legal privilege, including solicitor-client privilege.

Recommendation #22

It is recommended that the same procedure should apply to access to personal information under the proposed Privacy Act as applies to access to general information under the *Right to Information Act*.

Recommendation #23

It is recommended that a time limit of 30 days be imposed upon the head of a government body to respond to a request for access to personal information, but that an extension of 30 days should be available if it is impossible to respond to the request within the initial 30 day period.

Recommendation #24

It is recommended that an individual be entitled to request corrections to his or her personal information, and to have inaccurate information corrected.

Recommendation #25

It is recommended that, if a government body declines to make a correction, the government body must put an annotation on the information reflecting the nature of the individual's request, the fact that the request was denied and the reason for the denial.

Recommendation #26

It is recommended that a government body be subject to a reasonable requirement to communicate to third parties any correction of or annotation to personal information that the government body has previously disclosed to the third party.

Recommendation # 27

It is recommended that the Government of New Brunswick develop a personal information directory, listing the names and addresses of government bodies that hold personal information, the type of information each holds, the purpose for which that information was collected and is being used, and the categories of persons who have access to that information.

5 Supervision, Review and Appeal

Recommendation #28

It is recommended that a supervisory authority be appointed to fulfil the functions assigned to it by the proposed Privacy Act.

Recommendation #29

It is recommended that the role of supervisory authority of the proposed Privacy Act be placed with the Office of the Ombudsman.

Recommendation #30

It is recommended that the functions of the Ombudsman as the supervisory authority for the proposed Privacy Act be as follows:

(a) to receive complaints about the operation of the proposed Privacy Act;

(b) to conduct investigations, either on her own initiative or upon request, and to recommend resolutions to the complaints received;

(c) to conduct research and public education into issues of personal privacy;

(d) to review and comment on the privacy implications of legislative or administrative schemes or programs and their compliance with the proposed Privacy Act;

(e) to give advice and recommendations of general application to the head of a public body on matters respecting the rights or obligations of a head under the Act.

Recommendation #31

It is recommended that the supervisory authority have powers of investigation as provided under the *Ombudsman Act*.

Recommendation #32

It is recommended that

(a) in the case of a wrongful refusal of access to personal information under the proposed Privacy Act the individual's remedies should be the same as the remedies for wrongful refusal of access to other information under the *Right to Information Act*;

(b) for other complaints under the proposed Privacy Act the Ombudsman's powers under the *Ombudsman Act* should be the means of redress.

6 Internal Administration

Recommendation #33

It is recommended that in each government body a person be designated to be responsible for the operation and implementation of the Privacy Act.

Recommendation #34

It is recommended that a committee be established to give advice to deputy heads and privacy co-ordinators as to the implementation of the proposed

Privacy Act. This committee should operate for at least an initial period after the Act is proclaimed.

7 Offences and Penalties

Recommendation #35

It is recommended that an official of a government body who wilfully collects, uses, discloses or withholds personal information in violation of the proposed Privacy Act, or who destroys any records with the intent to evade a request for access to the records, commits an offence and is liable to a fine.

Recommendation #36

It is recommended that any person who, without lawful justification, obstructs or misleads the Ombudsman, or any person who applies for or requests access to or correction of personal information under false pretences, commits an offence and is liable to a fine.

8 Regulation-Making Power

Recommendation #37

It is recommended that the proposed Privacy Act contain regulation-making power to cover the following matters:

(a) prescribing a list of departments, boards, commissions and other bodies that are to be considered "government bodies" for the purposes of the Act;

(b) prescribing a list of persons to be considered heads of government bodies for the purposes of the Act;

(c) respecting the procedure to be followed on an application for access or a request for correction of personal information, or respecting the procedure to be followed in making a complaint to the Ombudsman;

(d) prescribing the amount of fees and respecting the circumstances under which a head can waive a fee;

(e) respecting forms for use under the Act.

9 Transitional and Consequential

Recommendation #38

It is recommended that the *Right to Information Act* be amended to provide that the relationship of an individual to a government body vis-à-vis his or her own personal information, including access to that information, is governed by the proposed Privacy Act and not by the *Right to Information Act*.

Recommendation #39

It is recommended that section 6 of the *Right to Information Act* be amended to link the disclosure of third party personal information under that Act to the disclosure provisions of the proposed Privacy Act.

Recommendation #40

It is recommended that the definition of "personal information" in the *Right to Information Act* be amended to match the definition of personal information proposed in recommendation #4.

Recommendation #41

It is recommended that the *Archives Act* be amended to ensure that personal information is dealt with under that Act in a manner that is consistent with the *Right to Information Act* and the proposed Privacy Act, but which recognizes the special considerations that apply in relation to archival material.